Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Jyothsnaa SIVARAMAN

Primitive roots for Pjateckii-Šapiro primes

Tome 33, nº 1 (2021), p. 83-94.

<http://jtnb.centre-mersenne.org/item?id=JTNB_2021__33_1_83_0>

Journal de Théorie des Nombres
de Bordeaux **33** (2021), 83–94

Primitive roots for Pjateckii-Šapiro primes

par Jyothsnaa SIVARAMAN

Résumé. Pour tout nombre réel positif non entier c, la suite $(\lfloor n^c \rfloor)_n$ est appelée suite de Pjateckii-Šapiro. Étant donné un nombre réel c dans l'intervalle $\left(1, \frac{11}{12}\right)$, on a une formule asymptotique pour le nombre de nombres premiers de cette suite qui sont au plus égaux à x. Nous utilisons la méthode de Gupta et Murty pour étudier le problème d'Artin pour ces nombres premiers. Nous démontrons que, bien que l'ensemble de ces nombres premiers a une densité relative nulle pour c donné, il existe des entiers positifs qui sont des racines primitives pour une infinité de nombres premiers de Pjateckii-Šapiro pour tout c fixé dans l'intervalle $\left(1, \frac{\sqrt{77}}{7} - \frac{1}{4}\right)$.

Abstract. For any non-integral positive real number c, any sequence $(\lfloor n^c \rfloor)_n$ is called a Pjateckii-Šapiro sequence. Given a real number c in the interval $\left(1, \frac{12}{11}\right)$, it is known that the number of primes in this sequence up to x has an asymptotic formula. We would like to use the techniques of Gupta and Murty to study Artin's problems for such primes. We will prove that even though the set of Pjateckii-Šapiro primes is of density zero for a fixed c, one can show that there exist natural numbers which are primitive roots for infinitely many Pjateckii-Šapiro primes for any fixed c in the interval $\left(1, \frac{\sqrt{77}}{7} - \frac{1}{4}\right)$.

1. Introduction

The study of prime producing polynomials in one variable is one that has attracted a lot of attention. Dirichlet's theorem on primes in arithmetic progressions supplies a satisfactory answer to this problem in the case of linear polynomials. However there has been little progress even in the case of quadratic polynomials. In 1953, Pjateckii-Šapiro studied a problem that may in some sense be considered as an intermediate step towards the quadratic case. For a non-integral positive real c, let

$$P_c(x) = \{p \leq x : p = \lfloor n^c \rfloor\} \tag{1.1}$$

where $\lfloor n \rfloor$ is used to denote the integral part of n. Such primes will be referred to in this paper as Pjateckii-Šapiro primes. Pjateckii-Šapiro ([12])

Manuscrit reçu le 26 janvier 2020, révisé le 16 janvier 2021, accepté le 1er février 2021.
2020 *Mathematics Subject Classification.* 11A07, 11N05, 11N35, 11N36.
Mots-clefs. Primitive roots, Pjateckii-Šapiro sequence, primes, sieve methods.

proved that for $c \in (1, 12/11)$, the number of such primes with p up to x (denoted $\pi_c(x)$) is asymptotic to

$$\frac{x^{\frac{1}{c}}}{\log x}.$$

A lot of work has gone into extending the range of c for which such an asymptotic formula is valid. For further reference in this regard the reader may look at [5, 7, 8, 10, 13, 14]. We are interested in something slightly different. In 1973, Leitmann and Wolke [9] proved that the number of Pjateckii-Šapiro primes in an arithmetic progression modulo q is asymptotic to

$$\frac{x^{\frac{1}{c}}}{\phi(q)\log x}.$$

We observe that such a property immediately allows the application of sieve methods to sets containing linear forms in Pjateckii-Šapiro primes. This brings us to the developments regarding a famous conjecture in mathematics, Artin's primitive root conjecture.

In 1927, Artin conjectured that every number a other than ± 1 or perfect squares is a primitive root for infinitely many primes. In 1967, Hooley [6] proved this under the extended Riemann hypothesis. In fact he proved that such an a is a primitive root for a positive density of primes, where this density is less than 1. In 1984, Gupta and Murty [3] showed unconditionally the existence of an $a \in \mathbb{N}$ and a $\delta > 0$ such that a is a primitive root mod p for atleast $\frac{\delta x}{\log^2 x}$ primes upto x. This was done using techniques of sieve methods and linear algebra.

We would like to prove a similar theorem by restricting our set of primes to the Pjateckii-Šapiro primes. A crucial ingredient of Gupta and Murty's proof is a result of Fouvry and Iwaniec [2]. However due to the absence of such techniques for Pjateckii-Šapiro primes we will prove our result based on a Bombieri–Vinogradov type theorem for Pjateckii-Šapiro primes [11]. We state our result precisely below.

Theorem 1. *For every real number $c \in (1, \frac{\sqrt{77}}{7} - \frac{1}{4})$, there exists a natural number a which is a primitive root for infinitely many primes in the sequence $(\lfloor n^c \rfloor)_n$.*

In the following section, we will introduce some preliminaries required to prove the above theorem and then move on to the proof in the subsequent section.

2. Preliminaries

We begin with some notation required for the sieve-theoretic arguments.

Let $\mathcal{P}$ be a subset of the set of rational primes, z be a real number and

$$\mathcal{P}(z) := \prod_{\substack{p\le z\\ p\in\mathcal{P}}} p. \tag{2.1}$$

Given a subset of non negative integers $\mathcal{A}$, let $\mathcal{A}_q := \{a \in \mathcal{A} : q|a\}$, where q is a natural number. In the sequel, ω is a multiplicative function, q is a square free natural number with all its prime divisors in $\mathcal{P}$ and r_q is as defined by (2.2):

$$|\mathcal{A}_q| = \frac{\omega(q)}{q}|\mathcal{A}| + r_q. \tag{2.2}$$

Set

$$V(z) = \prod_{\substack{p<z\\ p\in\mathcal{P}}} \left(1 - \frac{\omega(p)}{p}\right) \tag{2.3}$$

and

$$S(\mathcal{A},\mathcal{P},z) = \{a \in \mathcal{A} : (a,\mathcal{P}(z)) = 1\}, \tag{2.4}$$

where $(a,\mathcal{P}(z))$ denotes the gcd of a and $\mathcal{P}(z)$.

Theorem 2 (Halberstam and Richert (see [4, p. 236]))**.** *Let $\mathcal{P}$ be a subset of the set of rational primes, z be a real number and $\mathcal{P}(z), \omega, r_q, V(z)$ and $S(\mathcal{A},\mathcal{P},z)$ be as in* (2.1), (2.2), (2.3) *and* (2.4)*. Suppose that*

(a) *there exists a constant $A_1 \ge 1$ such that*

$$0 \le \frac{\omega(p)}{p} \le 1 - \frac{1}{A_1}$$

for all $p \in \mathcal{P}$;

(b) *there exist constants L and A_2, independent of z such that for any integer g_1 with $2 \le g_1 \le z$ one has*

$$-L \le \sum_{\substack{g_1\le p\le z\\ p\in\mathcal{P}}} \frac{\omega(p)\log p}{p} - \log\left(\frac{z}{g_1}\right) \le A_2;$$

(c) *there exists a real number α with $0 < \alpha \le 1$ such that*

$$\sum_{\substack{q|\mathcal{P}(z)\\ q<\frac{X^\alpha}{\log^F X}}} \mu^2(q)3^{\nu(q)}|r_q| \le \frac{G_1 X}{\log^2 X}$$

for some positive constants F and G_1. Here μ is the Möbius function and $\nu(q)$ denotes the number of distinct prime divisors of q.

Then for $X \geq z$, one has

$$S(\mathcal{A}, \mathcal{P}, z) \geq XV(z)\left\{g\left(\alpha\frac{\log X}{\log z}\right) - \frac{B}{\log^{1/14} X}\right\}.$$

Here g is a continuous function on $[2, \infty)$ satisfying

$$g(s) = 2e^{\gamma}\log(s-1)/s,$$

for $s \in [2, 4]$. Here γ is the Euler and Mascheroni constant and B is an absolute constant.

In order to estimate the term stated in (c) of the theorem above we will require a theorem of Deshouillers ([1]) and an analogue of the Bombieri Vinogradov theorem ([11]), both of which we state below.

Theorem 3 (Deshouillers ([1]))**.** *Let $c \in (1, 2)$ and let x be a real number. Let q and a be two integers such that $0 \leq a < q \leq x^c$. One has*

$$\left|N_c(x; q, a) - \frac{x}{q}\right| \ll_c \frac{x^{(c+1)/3}}{q^{1/3}}$$

where $N_c(x; q, a) = |\{n \leq x : \lfloor n^c \rfloor \equiv a \bmod q\}|$.

The above theorem implies that for $0 \leq a < q \leq x^{\frac{2-c}{2c}}$

$$N_c((x+1)^{1/c}, q, a) \ll_c \frac{x^{1/c}}{q} + \frac{x^{\frac{c+1}{3c}}}{q^{1/3}} \ll \frac{x^{1/c}}{q}.$$

In particular, in this range we have

$$\left|\pi_c(x; q, a) - \frac{x^{1/c}}{\phi(q)\log(x)}\right| \leq N_c((x+1)^{1/c}; q, a) + \frac{x^{1/c}}{\phi(q)\log(x)} \tag{2.5}$$

$$\ll_c \frac{x^{1/c}}{\phi(q)}, \tag{2.6}$$

where $\pi_c(x; d, a) := |\{p \leq x : p = \lfloor n^c \rfloor, p \equiv a \bmod q\}|$. This bound will be applied in Section 3 in order to bound the error term in the sieve. We now state the following result of Lu, as referred to in the introduction.

Theorem 4 (Lu ([11]))**.** *Let $\epsilon > 0$ and $\xi = \frac{13/c-12}{4} - \epsilon$, where $1 < c < \frac{13}{12}$. Then for fixed integer $a \neq 0$, we have*

$$\sum_{\substack{d \leq x^{\xi} \\ (d,a)=1}} \left|\pi_c(x, d, a) - \frac{1}{\phi(d)}\pi_c(x)\right| \ll \frac{x^{1/c}}{\log^A x},$$

where A is an arbitrary positive real number.

Finally we state the well known Gupta–Murty lemma.

Lemma 5 (Gupta and Murty ([3])). *Suppose that* $q_1, \dots, q_n$ *are a set of* n *distinct rational primes. Let* $\Gamma = \{q_1^{a_1} \dots q_n^{a_n} : a_i \in \mathbb{N}\}$ *and* $\Gamma_p = \{a \bmod p : a \in \Gamma\}$. *Then*

$$|\{p : p \text{ is a rational prime and } |\Gamma_p| \le y\}| \ll y^{\frac{n+1}{n}}.$$

With this we conclude our section on the preliminaries and move on to the proof of our theorems.

3. Proof of theorem

Before we begin proving the theorem, let us fix some notation for the sake of convenience. Let η be equal to $\frac{13/c-12}{16}$ and let $n = \lfloor \eta^{-1} \rfloor$. Further let $q_1, \dots, q_n$ be n distinct odd primes with $q_1 \equiv 1 \bmod 4$. Since the value of c required for Theorem 1 is in $(1, 1.004)$, in this case $n = 16$.

Theorem 6. *For* q_1 *as chosen and a* $c \in \left(1, \frac{\sqrt{77}}{7} - \frac{1}{4}\right)$ *and let*

$$T(x) := \left\{ p - 1 \le x : \begin{array}{l} \left(\frac{q_1}{p}\right) = -1, \ p = \lfloor n^c \rfloor, \\ \text{any odd prime dividing } p-1 \text{ is larger than } x^\eta \end{array} \right\}.$$

Then, we have

$$|T(x)| \gg \frac{x^{1/c}}{\log^2 x}.$$

Proof. By the law of quadratic reciprocity, we can choose an $a \bmod q_1$ such that $p \equiv a \bmod q_1$ implies that q_1 is a quadratic non-residue mod p. Let

$$\mathcal{A} = \{p - 1 \le x : p \equiv a \bmod q_1, p = \lfloor n^c \rfloor\}.$$

The choice of p will ensure that q_1 cannot divide $p-1$. Let $\mathcal{P} = \{p : p \ne 2, q_1\}$. By [9] we have that $X = \frac{x^{1/c}}{\phi(q_1)\log x}$. For $p \in \mathcal{P}$, we define $\omega(p) = \frac{p}{p-1}$. Condition (a) of Theorem 2 will be trivially satisfied by choosing $A_1 = 2$. To check condition (b), for any $2 \le g_1 \le z$ we consider

$$\sum_{\substack{g_1 \le p \le z \\ p \in \mathcal{P}}} \frac{\omega(p) \log p}{p} = \sum_{g_1 \le p \le z} \frac{\frac{p}{p-1} \log p}{p} - \sum_{\substack{g_1 \le p \le z, \\ p | 2q_1}} \frac{\frac{p}{p-1} \log p}{p}.$$

Since the second term in the above equality is bounded by a constant, we have

$$\begin{aligned}
&\sum_{\substack{g_1 \le p \le z \\ p \in \mathcal{P}}} \frac{\omega(p)\log p}{p} - \log(z/g_1) \\
&\quad = \sum_{g_1 \le p \le z} \frac{\log p}{p} + \sum_{g_1 \le p \le z} \frac{\log p}{p(p-1)} - \log(z/g_1) + O(1) \\
&\quad = O(1).
\end{aligned}$$

On observing condition (c), one notes that the factor $3^{\nu(q)}$ is not present in the usual versions of the Bombieri–Vinogradov theorem. But Cauchy–Schwarz permits us to treat this sum as soon as one has a Bombieri–Vinogradov theorem and an upper bound for r_q in which not more than a power of log is lost. The Bombieri–Vinogradov theorem is as stated in Theorem 4 ([11]), and the upper bound is as obtained from (2.5) (comment following Theorem 3 ([1])).

$$\sum{}' 3^{\nu(q)}|r_q| \le \sqrt{\sum{}' 9^{\nu(q)}|r_q|}\sqrt{\sum{}'|r_q|}$$

where the sum $\sum'$ is over the integers q which are less than $x^{2\eta+\epsilon}$ (for ϵ sufficiently small) and divide $\mathcal{P}(z)$. Here $\mathcal{P}(z)$ is defined in (2.1). Note that since we have $c < 3/2$ and $q < x^{1/6}$, (2.5) is applicable. Therefore, for any $q|\mathcal{P}(z)$, we have by [11], and by the comment after Theorem 3 ([1], (2.5))

$$\sum{}' |r_q| \ll \frac{x^{\frac{1}{c}}}{\log^F x} \text{ and } |r_q| \ll \frac{x^{1/c}}{\phi(q)}$$

$$\begin{aligned}
\text{and} \quad \sum{}' \frac{9^{\nu(q)}}{\phi(q)} &\le \sum_{\substack{q < x^{2\eta+\epsilon} \\ q \text{ square free}}} \frac{9^{\nu(q)}}{\phi(q)} \\
&\le \prod_{p < x^{2\eta+\epsilon}} \left(1 + \frac{1}{p-1}\right)^9 \\
&\le \prod_{p < x^{2\eta+\epsilon}} \left(1 - \frac{1}{p}\right)^{-9} \ll \log^9 x,
\end{aligned}$$

where in the last step, we have used Merten's theorem. Hence

$$\sum{}' 3^{\nu(q)}|r_q| \ll \frac{X}{\log^2 X}.$$

We now observe that for $z = x^\eta$, $\alpha = c(2\eta + \epsilon)$,

$$\frac{2\eta + \epsilon}{\eta} \cdot \frac{\log x - c \cdot \log(\phi(q_1)\log x)}{\log x} \le 4.$$

Further for $\delta > 0$ sufficiently small and x is sufficiently large

$$\frac{2\eta+\epsilon}{\eta} \cdot \frac{\log x - c \cdot \log(\phi(q_1)\log x)}{\log x} \geq \frac{2\eta+\epsilon}{\eta} \cdot (1-\delta) > 2.$$

Therefore, now applying Theorem 2 and Merten's theorem we have

$$S(\mathcal{A}, \mathcal{P}, x^{\eta}) \gg \frac{x^{1/c}}{\log^2 x}. \qquad \square$$

Theorem 7. *Consider the primes $q_1, \ldots, q_n$. Let Γ_p be as in Lemma 5. For $c \in (1, \frac{\sqrt{77}}{7} - \frac{1}{4})$, the number of p with $p - 1 \in T(x)$ such that $\mathbf{F}_p^* = \langle q_1 \bmod p, \ldots, q_n \bmod p\rangle$ is atleast $\frac{\delta x^{1/c}}{\log^2 x}$ for some positive δ and x sufficiently large.*

Proof. If $(\mathbb{Z}/p\mathbb{Z})^* \neq \Gamma_p$, then let i be the index of Γ_p in $(\mathbb{Z}/p\mathbb{Z})^*$. Since $p - 1 \in T(x)$, this implies that $2 \mid i$ or $i > x^{\eta}$. The squares modulo p form an index two subgroup mod p. Since i divides $[(\mathbb{Z}/p\mathbb{Z})^* : \langle q_1\rangle \bmod p]$ and $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic, if $2 \mid i$, then q_1 is a quadratic residue modulo p but $\left(\frac{q_1}{p}\right) = -1$. Therefore $i > x^{\eta}$. This implies that $|\Gamma_p| \leq x^{1-\eta}$. Therefore by Lemma 5, we have

$$\{p : |\Gamma_p| \leq x^{1-\eta}\} \ll x^{1-(\eta)^2}$$

For c sufficiently close to one this term is $o\left(\frac{x^{1/c}}{\log^2 x}\right)$. In order to compute such a c, we consider the inequality

$$1 - \left(\frac{13/c - 12}{16}\right)^2 < \frac{1}{c}.$$

This is equivalent to $112c^2 + 56c - 169 < 0$ which holds for all $c \in (1, \frac{\sqrt{77}}{7} - \frac{1}{4})$. $\square$

Theorem 8. *Given a set S of $2^{n-2} \times 7$ tuples each consisting of n entries in $\mathbb{Z}$ satisfying;*

(a) $(u_1, u_2, \ldots, u_n) \not\equiv (0, 0, \ldots, 0) \bmod 2$ *for all* $(u_1, u_2, \ldots, u_n) \in S$*;*
(b) *for any element $(u_1, u_2, \ldots, u_n)$ of S there is atmost one other element $(v_1, v_2, \ldots, v_n)$ of S such that $(u_1, u_2, \ldots, u_n) \equiv (v_1, v_2, \ldots, v_n) \bmod 2$;*
(c) *for any $n - 1$ dimensional subspace V of $(\mathbb{Z}/2\mathbb{Z})^n$, any family of n elements of the set S_V are linearly independent, where*

$$S_V := \left\{(u_1, u_2, \ldots, u_n) \in S : \begin{array}{r} (u_1, u_2, \ldots, u_n) \not\equiv (v_1, v_2, \ldots, v_n) \bmod 2 \\ \textit{for all } (v_1, v_2, \ldots, v_n) \in V \end{array}\right\}.$$

Then there exists a $(u_1, u_2, \ldots, u_n)$ in S such that $q_1^{u_1} \cdots q_n^{u_n}$ is a primitive root for at least $\frac{\delta' x^{\frac{1}{c}}}{\log^2 x}$ elements of $T(x)$ for some positive constant δ' and x sufficiently large.

Proof. Let p_0 be a prime such that $p_0 - 1 \in T(x)$ and $\mathbf{F}_{p_0}^* = \langle q_1 \bmod p_0, \ldots, q_n \bmod p_0 \rangle$. Let g be a primitive root modulo p_0. Then for all $1 \leq i \leq n$ we have e_i such that

$$q_i \equiv g^{e_i} \bmod p_0.$$

By the choice of p_0, we have

$$(e_1, e_2, \ldots, e_n, p_0 - 1) = 1.$$

Therefore $(e_1, e_2, \ldots, e_n) \not\equiv (0, 0, \ldots, 0) \bmod 2$. Now let V be the orthogonal complement space of this vector on reading modulo 2. We now consider S_V. By condition (b), the cardinality of S_V is at least

$$(7 \times 2^{n-2}) - 2(2^{n-1} - 1) = (3 \times 2^{n-2}) + 2.$$

Further, we observe that $q_1^{u_1} \ldots q_n^{u_n}$ is a primitive root modulo p_0 if and only if

$$\left(\sum_{i=1}^{n} u_i e_i, p_0 - 1 \right) = 1.$$

Since the elements of S_V are not in V on reading modulo 2, it follows that for all $(u_1, u_2, \ldots u_n)$ in S_V,

$$2 \nmid \sum_{i=1}^{n} u_i e_i.$$

Now consider the matrix of any n elements from S_V. By our hypothesis the determinant is non zero. However observe that

$$\begin{bmatrix} u_1^{(1)} & u_2^{(1)} & \ldots & u_n^{(1)} \\ \vdots & & & \\ u_1^{(n)} & u_2^{(n)} & \ldots & u_n^{(n)} \end{bmatrix} \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix} = \begin{bmatrix} \sum u_i^{(1)} e_i \\ \vdots \\ \sum u_i^{(n)} e_i \end{bmatrix}. \tag{3.1}$$

Discarding finitely many possible values of p_0, we can assume that the odd primes dividing $p_0 - 1$ are coprime to the determinant of the above n by n matrix. Now each divisor of $p_0 - 1$ can divide atmost $n - 1$ of the entries on the right hand side of (3.1). This is because of the initial condition that $(e_1, e_2, \ldots, e_n, p_0 - 1) = 1$. Since $p_0 - 1$ has atmost n prime divisors other than 2 and each divisor of $p_0 - 1$ can divide atmost $n - 1$ elements of the form $\sum u_i e_i$ for $(u_1, u_2, \ldots u_n) \in S_V$. We can now say that there are

$$(3 \times 2^{n-2}) + 2 - n(n-1)$$

elements remaining in S_V such that for any point $(u_1, u_2, \ldots, u_n)$ left in S_V, the term given by $q_1^{u_1} \ldots q_n^{u_n}$ is a primitive root for p_0. This shows that for p_0 as chosen above, we have the existence of a primitive root of the form $q_1^{u_1} \ldots q_n^{u_n}$ for some $(u_1, u_2, \ldots, u_n) \in S$. But since there are only finitely many points in S, and $\delta x^{1/c} / \log^2 x$ possible choices for p_0 (by Theorem 7), we have a primitive root for at least $\delta' x^{1/c}/\log^2 x$ primes of $T(x)$ for some positive δ'. $\square$

We now need to prove that a set with the properties of S exists. To do so, we begin with the following lemma.

Lemma 9. *Given any N there exists a set of $7N$ vectors in $\mathbb{Z}^3$ such that*

(a) *any three of these vectors are linearly independent over $\mathbb{R}$;*

(b) *for any non-zero congruence class modulo 2, exactly N vectors belong to this class, i.e.*

$$(a, b, c) \equiv (a_1, b_1, c_1) \bmod 2$$

for exactly N vectors in this set.

Proof. We will prove the same by induction on N. For $N = 1$ we follow Gupta and Murty and consider the set

$$S_1 := \{(1,0,2), (2,1,0), (0,2,1), (1,3,0), (0,1,3), (3,0,1), (1,1,1)\}.$$

It is easy to check that any three of these vectors are linearly independent. Now suppose that we have the set for $N-1$ (denoted S_{N-1}, consisting of $7(N-1)$ vectors satisfying (a) and (b)). To construct the set for N, consider one of the non-zero congruence classes modulo 2 in $(\mathbb{Z}/2\mathbb{Z})^3$. Let this be represented by $\overline{v}$. Consider the sublattice of $\mathbb{Z}^3$ given by all the vectors congruent to $(0,0,0)$ and $\overline{v}$. Since this sublattice contains a set of three linearly independent elements, it cannot be contained in a plane. Therefore it is of rank 3. Now observe that no rank 3 sublattice of $\mathbb{Z}^3$ can be written as a union of finitely many rank two sublattices. For each non-trivial class $\overline{v}$, by our induction hypothesis, we already have S_{N-1} with $7(N-1)$ vectors satisfying the above two properties. So let us start with a vector in S_{N-1} which are congruent to $\overline{v}$ (Say w).

There exists a point in this lattice (given by w and the vectors congruent to (0,0,0)) which is not contained in the plane generated by any two vectors in S_{N-1}. If this vector, say u, is congruent to $\overline{v}$ then our construction is complete. If not, u is congruent to $(0,0,0)$. In the second case consider a vector in this lattice:

$$n_1 w + n_2 u$$

where n_1 is odd and it does not belong to the finitely many planes given by any two elements of S_{N-1}. This will now give us a vector congruent to $\overline{v}$ satisfying the linear independence condition. Similarly, we now add 6 more vectors (satisfying appropriate congruence conditions) by ensuring that each one does not belong to any of the planes spanned by any set of two vectors chosen before it. This completes the proof of the lemma. $\square$

Theorem 10. *Given any $n > 3$ there exists a set of $2^{n-2} \times 7$, n-tuples with entries in $\mathbb{Z}$, satisfying the hypothesis of Theorem 8.*

Proof. The proof proceeds by induction. We provide below the first step of the induction process which can be seen as generic. Choose a set of $2^{n-2} \times 7$ vectors of dimension 3 (denoted by S_{n-2}) using Lemma 9. Let M be an integer greater than the maximum of the absolute value of the determinant of any three vectors in S_{n-2}. By our choice of these vectors, each class $\bar{a}$ of $(\mathbb{Z}/2\mathbb{Z})^3$ except the one corresponding to $(0,0,0)$ contains exactly 2^{n-2} vectors of this set. We denote this set of 2^{n-2} vectors by $T_{\bar{a}}$. We now extend these to four dimensional vectors by adjoining a power of M or $M+1$ in the following manner.

In each $T_{\bar{a}}$, we extend 2^{n-3} vectors by adjoining distinct powers of M, such that as we vary the classes $\bar{a}$, the powers are all distinct. Let the highest power of M thus assigned be x.

For the other 2^{n-3} vectors in each $T_{\bar{a}}$ we adjoin powers (strictly greater than x) of $M+1$, once again we ensure that the powers are distinct on varying $\bar{a}$.

This will ensure that exactly 2^{n-3} extensions are congruent modulo 2 and that any four of these 4-dimensional vectors are linearly independent over $\mathbb{R}$. The condition (c) of the statement comes from the following observation. Consider the matrix

$$L := \begin{bmatrix} u_1^{(1)} & u_2^{(1)} & u_3^{(1)} & u_4^{(1)} \\ u_1^{(2)} & u_2^{(2)} & u_3^{(2)} & u_4^{(2)} \\ u_1^{(3)} & u_2^{(3)} & u_3^{(3)} & u_4^{(3)} \\ X_1 & X_2 & X_3 & X_4 \end{bmatrix}$$

where the X_i is either a power of M or $M+1$ as the case may be.

Suppose that the cofactor to the X_i is given by α_i. Then the determinant of L is given by

$$\det(L) = \alpha_1 X_1 + \alpha_2 X_2 + \alpha_3 X_3 + \alpha_4 X_4$$

where $|\alpha_i| < M$ cannot be zero. We provide below the argument in the most general case. Suppose that $|\alpha_i| < M$ and

$$\begin{aligned} K &:= \alpha_1 M^{m_1} + \alpha_2 M^{m_2} + \cdots + \alpha_l M^{m_l} + \alpha_{l+1}(M+1)^{m_{l+1}} + \cdots + \alpha_p (M+1)^{m_p} \\ &= \alpha_1 M^{m_1} + M^{m_2}(\alpha_2 + \cdots + \alpha_l M^{m_l - m_2}) \\ &\qquad + (M+1)^{m_{l+1}}(\alpha_{l+1} + \cdots + \alpha_p (M+1)^{m_p - m_{l+1}}). \end{aligned}$$

It follows that if there is at least one term with $M+1$ then

$$\begin{aligned} &|M^{m_2}(\alpha_2 + \cdots + \alpha_l M^{m_l - m_2}) + (M+1)^{m_{l+1}}(\alpha_{l+1} + \cdots + \alpha_p (M+1)^{m_p - m_{l+1}})| \\ &\qquad > (M+1)^{m_{l+1}} - M^{m_l+1} - \ldots M^{m_2+1} > M^{m_2} \end{aligned}$$

Since $|\alpha_1 M^{m_1}| < M^{m_2}$, it follows that K is non-zero. For the d-th stage in the induction process:

(a) We start with the set (Q) of $(d+2)$-dimensional vectors of cardinality $2^{n-2} \times 7$. This set has the property that any $d+2$ vectors are linearly independent.

(b) Each $\bar{a} \in (\mathbb{Z}/2\mathbb{Z})^{d+2}$ which occurs in Q, corresponds to exactly 2^{n-1-d} vectors.

(c) Let N be an integer greater than the absolute value of the determinant of any $d+2$ vectors from the initial set. For each $\bar{a} \in (\mathbb{Z}/2\mathbb{Z})^{d+2}$ which occurs in Q, extend 2^{n-2-d} vectors by appending distinct powers of N such that the powers are distinct as we vary over $\bar{a}$ occuring in Q. Suppose that the highest such power is x. Extend the other 2^{n-2-d} vectors by appending distinct powers (strictly greater than x) of $N+1$, again distinct as we vary over $\bar{a}$ occuring in Q.

(d) On constructing a matrix from $d+3$ vectors of this new set, the above argument shows that these are all linearly independent.

Repeating this process $n-3$ times we get a set of $2^{n-2} \times 7$ vectors satisfying the hypothesis of Theorem 8. ☐

Acknowledgments. The author would like to thank the referee for the helpful comments and suggestions.

References

[1] J.-M. Deshouillers, "A remark on cube-free numbers in Segal–Piatestki-Shapiro sequences", *Hardy-Ramanujan J.* **41** (2019), p. 127-132.

[2] É. Fouvry & H. Iwaniec, "Primes in arithmetic progressions", *Acta Arith.* **42** (1983), no. 2, p. 197-218.

[3] R. Gupta & M. R. Murty, "A remark on Artin's conjecture", *Invent. Math.* **78** (1984), no. 1, p. 127-130.

[4] H. Halberstam & H.-E. Richert, *Sieve methods*, London Mathematical Society Monographs, vol. 4, Academic Press Inc., 1974.

[5] D. R. Heath-Brown, "The Pjateckii-Šapiro prime number theorem", *J. Number Theory* **16** (1983), p. 242-266.

[6] C. Hooley, "On Artin's conjecture", *J. Reine Angew. Math.* **225** (1967), p. 209-220.

[7] C. Jia, "On Pjateckiĭ-Šapiro prime number theorem", *Chin. Ann. Math., Ser. B* **15** (1994), no. 1, p. 9-22.

[8] G. A. Kolesnik, "The distribution of primes in sequences of the form $[n^c]$", *Mat. Zametki* **2** (1972), p. 117-128.

[9] D. Leitmann & D. Wolke, "Primzahlen der Gestalt $[n^\Gamma]$ in arithmetischen Progressionen", *Arch. Math.* **25** (1974), p. 492-494.

[10] H. Q. Liu & J. Rivat, "On the Pjateckii-Šapiro prime number theorem", *Bull. Lond. Math. Soc.* **24** (1992), no. 2, p. 143-147.

[11] Y. M. Lu, "An additive problem on Pjateckii-Šapiro primes", *Acta Math. Sin., Engl. Ser.* **34** (2018), no. 2, p. 255-264.

[12] I. I. Pjateckii-Šapiro, "On the distribution of prime numbers in sequences of the form $[f(n)]$", *Mat. Sb.* **33** (1953), p. 559-566.

[13] J. Rivat & P. Sargos, "Nombres premiers de la forme $\lfloor n^c \rfloor$", *Can. J. Math.* **53** (2001), no. 2, p. 414-433.

[14] J. RIVAT & J. WU, "Prime numbers of the form $\lfloor n^c \rfloor$", *Glasg. Math. J.* **43** (2001), no. 2, p. 237-254.

Jyothsnaa SIVARAMAN
University of Toronto, Toronto
Ontario, Canada - M5T 3J1.
E-mail: jyothsnaa.sivaraman@utoronto.ca
E-mail: jyothsnaa.s@gmail.com