COLLOQUIUM MATHEMATICUM

VOL. 125 2011 NO. 1

CARMICHAEL NUMBERS COMPOSED OF PRIMES FROM A BEATTY SEQUENCE

BY

WILLIAM D. BANKS and AARON M. YEAGER (Columbia, MO)

Abstract. Let $\alpha, \beta \in \mathbb{R}$ be fixed with $\alpha > 1$, and suppose that α is irrational and of finite type. We show that there are infinitely many Carmichael numbers composed solely of primes from the non-homogeneous Beatty sequence $\mathscr{B}_{\alpha,\beta} = (\lfloor \alpha n + \beta \rfloor)_{n=1}^{\infty}$. We conjecture that the same result holds true when α is an irrational number of infinite type.

1. Introduction. If N is a prime number, *Fermat's little theorem* asserts that

$$a^N \equiv a \pmod{N} \quad \text{for all } a \in \mathbb{Z}.$$

Around 1910, Robert Carmichael initiated the study of composite numbers N with the same property, which are now known as *Carmichael numbers*. In 1994 the existence of infinitely many Carmichael numbers was first established by Alford, Granville and Pomerance [1]. In recent years, using variants of the method of [1], several arithmetically defined classes of Carmichael numbers have been shown to contain infinitely many members; see [3, 4, 5, 9].

In the present note we consider the problem of constructing Carmichael numbers that are composed of primes from a Beatty sequence. Recall that for fixed $\alpha, \beta \in \mathbb{R}$ the associated *non-homogeneous Beatty sequence* is the sequence of integers defined by

$$\mathscr{B}_{\alpha,\beta} = (\lfloor \alpha n + \beta \rfloor)_{n \in \mathbb{Z}}.$$

Here we consider only Beatty sequences $\mathcal{B}_{\alpha,\beta}$ with α irrational and $\alpha > 1$ (note that for any irrational $\alpha \in (0,1)$ the set $\mathcal{B}_{\alpha,\beta}$ contains all large natural numbers, so the construction given in [1] already produces infinitely many Carmichael numbers composed of primes from $\mathcal{B}_{\alpha,\beta}$). For technical reasons, we assume that the *type* $\tau = \tau(\alpha)$ of the irrational number α is finite, where

$$\tau = \sup\{t \in \mathbb{R} : \liminf_{n \to \infty} n^t [\![\alpha n]\!] = 0\}.$$

Note that the theorems of Khinchin [10] and of Roth [13, 14] assert that $\tau = 1$ for almost all real numbers (in the sense of the Lebesgue measure) and for all irrational algebraic numbers α, respectively; see also [7, 15].

2010 *Mathematics Subject Classification*: Primary 11N25; Secondary 11N13, 11B83.
Key words and phrases: Carmichael numbers, Beatty sequences.

DOI: 10.4064/cm125-1-9

THEOREM 1. *Let $\alpha, \beta \in \mathbb{R}$ with $\alpha > 1$, and suppose that α is irrational and of finite type. Then there are infinitely many Carmichael numbers composed solely of primes from the Beatty sequence $\mathscr{B}_{\alpha,\beta}$.*

A quantitative version of this result is given in §4; see Theorem 3. To prove Theorem 1, we show that when α is of finite type, the set of primes in a Beatty sequence is sufficiently well-distributed over arithmetic progressions that one can construct Carmichael numbers from such primes using an adaptation of the method of [1]. To this end, we extend various results and techniques of Banks and Shparlinski [6].

For irrational numbers α of infinite type, the approach described above fails; however, assuming a certain natural extension of Dickson's k-tuplet conjecture (see [8]), the following conjecture can be established conditionally in many cases.

CONJECTURE. *The conclusion of Theorem 1 also holds when α is an irrational number of infinite type.*

2. Preliminaries

2.1. General notation. The notation $[\![t]\!]$ is used to denote the distance from the real number t to the nearest integer; that is,

$$[\![t]\!] = \min_{n \in \mathbb{Z}} |t - n| \quad (t \in \mathbb{R}).$$

We denote by $\lfloor t \rfloor$ and $\{t\}$ the greatest integer $\le t$ and the fractional part of t, respectively. We also put $e(t) = e^{2\pi i t}$ for all $t \in \mathbb{R}$. As usual, we use $\Lambda(\cdot)$ and $\varphi(\cdot)$ to denote the von Mangoldt and Euler functions, respectively.

Throughout the paper, the implied constants in symbols O, $\ll$ and $\gg$ may depend on the parameters α, β and ε but are absolute otherwise. We recall that for functions F and G the notations $F \ll G$, $G \gg F$ and $F = O(G)$ are all equivalent to the statement that the inequality $|F| \le C|G|$ holds for some constant $C > 0$.

2.2. Discrepancy. Recall that the *discrepancy* $D(M)$ of a sequence of (not necessarily distinct) real numbers $a_1, \dots, a_M \in [0, 1)$ is defined by

$$D(M) = \sup_{\mathcal{I} \subseteq [0,1)} \left| \frac{V(\mathcal{I}, M)}{M} - |\mathcal{I}| \right|, \tag{1}$$

where the supremum is taken over all intervals $\mathcal{I}$ contained in $[0, 1)$, $V(\mathcal{I}, M)$ denotes the number of positive integers $m \le M$ such that $a_m \in \mathcal{I}$, and $|\mathcal{I}|$ denotes the length of the interval $\mathcal{I}$.

For every irrational number γ, the sequence of fractional parts $(\{n\gamma\})_{n=1}^{\infty}$ is uniformly distributed in $[0, 1)$ (see, e.g., [11, Chapter 1, Example 2.1]). In

the case that γ is of finite type, the following more precise statement holds (see [11, Chapter 2, Theorem 3.2]).

LEMMA 1. *Let γ be a fixed irrational number of finite type τ. Then, for every $\delta \in \mathbb{R}$, the discrepancy $D_{\gamma,\delta}(M)$ of the sequence $(\{\gamma m + \delta\})_{m=1}^{M}$ satisfies the bound*

$$D_{\gamma,\delta}(M) \le M^{-1/\tau+o(1)} \qquad (M \to \infty),$$

where the function implied by $o(\cdot)$ depends only on γ.

2.3. Numbers in a Beatty sequence. The following lemma provides a convenient characterization of the numbers which occur in a Beatty sequence $\mathscr{B}_{\alpha,\beta}$.

LEMMA 2. *Let $\alpha, \beta \in \mathbb{R}$ with $\alpha > 1$, and put $\gamma = \alpha^{-1}$, $\delta = \alpha^{-1}(1-\beta)$. Then $n \in \mathscr{B}_{\alpha,\beta}$ if and only if $\psi(\gamma n + \delta) = 1$, where $\psi = \psi_\alpha$ is the periodic function defined by*

$$\psi(t) = \begin{cases} 1 & \text{if } 0 < \{t\} \le \alpha^{-1}, \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

2.4. Sums with the von Mangoldt function. The next statement is a simplified and weakened version of a theorem of Balog and Perelli [2] (see also [12]).

LEMMA 3. *For an arbitrary real number θ and coprime integers c and d with $0 \le c < d$, we have the uniform bound*

$$\sum_{\substack{n \le x \\ n \equiv c \,(\mathrm{mod}\, d)}} \Lambda(n) e(\theta n) \ll (q^{-1/2}x + q^{1/2}x^{1/2} + x^{4/5})(\log x)^3$$

whenever the inequality $|\theta - a/q| \le 1/x$ holds with some real $x > 1$ and coprime integers a and $q \ge 1$.

As an application of Lemma 3 we derive the following statement, which is an explicit version of [6, Theorem 4.2].

LEMMA 4. *Let γ be an irrational number of finite type τ, and fix $A \in (0,1)$ and $\varepsilon > 0$. For any coprime integers c and d with $0 \le c < d$ and any non-zero integer k such that $|k| \le x^A$, the bound*

$$\sum_{\substack{n \le x \\ n \equiv c \,(\mathrm{mod}\, d)}} \Lambda(n) e(k\gamma n) \ll x^{\frac{A+2+1/\tau}{2+2/\tau}+\varepsilon} + x^{4/5}(\log x)^3$$

holds, where the implied constant depends only on the parameters α, β, A and ε.

Proof. It suffices to prove this for $\varepsilon \in (0, 1/3)$. Put

$$B = \frac{A+1}{1+1/\tau}, \qquad C = \frac{\tau(1+\varepsilon)}{1-\varepsilon\tau}, \qquad D = \frac{A+1}{1+1/\tau} + 2\varepsilon.$$

Note that $B \in (0,1)$ (since $\tau \ge 1$ for an irrational γ), $C \in (\tau, 2\tau)$, and

$$D = B + 2\varepsilon > B(1+\varepsilon) = \frac{A+1}{1+1/C},$$

which implies that

$$-A + C/D > 1 - D. \tag{3}$$

Since $C \in (\tau, 2\tau)$ and γ is of type τ, we have

$$[\![\gamma m]\!] \ge c_0 |m|^{-C} \quad (m \in \mathbb{Z},\ m \ne 0) \tag{4}$$

for some number $c_0 > 0$ that depends only on τ and ε.

Let a/q be the convergent in the continued fraction expansion of $k\gamma$ which has the largest denominator q not exceeding $c_0^{-1} x^D$; then

$$\left| k\gamma - \frac{a}{q} \right| \le \frac{1}{q c_0^{-1} x^D} = \frac{c_0}{q x^D}. \tag{5}$$

Multiplying by q and using (4) we have

$$c_0 x^{-D} \ge |qk\gamma - a| \ge [\![qk\gamma]\!] \ge c_0 |qk|^{-C}.$$

Since $|k| \le x^A$ it follows that $q \ge x^{-A+D/C}$. By (3) we have $q \ge c_0 x^{1-D}$ for all sufficiently large x, hence by (5) we see that $|k\gamma - a/q| \le 1/x$. Applying Lemma 3 with $\theta = k\gamma$, and taking into account our choice of D and the inequalities $c_0 x^{1-D} \le q \le c_0^{-1} x^D$, we derive the stated bound. ∎

3. Beatty primes in arithmetic progressions. For the remainder of the paper, let $\alpha, \beta \in \mathbb{R}$ be fixed with $\alpha > 1$, and assume that α is irrational. The following statement provides an explicit version of [6, Theorem 5.4].

THEOREM 2. *If α is of finite type $\tau = \tau(\alpha)$, then for any fixed $\varepsilon > 0$ we have*

$$\sum_{\substack{n \le x,\ n \in \mathscr{B}_{\alpha,\beta} \\ n \equiv c \,(\mathrm{mod}\, d)}} \Lambda(n) = \frac{1}{\alpha} \sum_{\substack{n \le x \\ n \equiv c \,(\mathrm{mod}\, d)}} \Lambda(n) + O(x^{1-1/(4\tau+2)+\varepsilon}), \tag{6}$$

where the implied constant depends only on the parameters α, β and ε.

Proof. Let $F(x; d, c)$ denote the left side of (6), and let $\psi = \psi_\alpha$ be defined by (2). In view of Lemma 2 we have

$$F(x; d, c) = \sum_{\substack{n \le x \\ n \equiv c \,(\mathrm{mod}\, d)}} \Lambda(n) \psi(\gamma n + \delta),$$

where $\gamma = \alpha^{-1}$ and $\delta = \alpha^{-1}(1-\beta)$. Note that α and γ are of the same type, that is, $\tau(\alpha) = \tau(\gamma)$.

By a classical result of Vinogradov (see [16, Chapter I, Lemma 12]), for any Δ such that $0 < \Delta < \frac{1}{8}$ and $\Delta \le \frac{1}{2}\min\{\gamma, 1-\gamma\}$, there is a real-valued function Ψ with the following properties:

(i) Ψ is periodic with period one;
(ii) $0 \le \Psi(t) \le 1$ for all $t \in \mathbb{R}$;
(iii) $\Psi(t) = \psi(t)$ if $\Delta \le \{t\} \le \gamma - \Delta$ or if $\gamma + \Delta \le \{t\} \le 1 - \Delta$;
(iv) $\Psi(t) = \sum_{k\in\mathbb{Z}} g(k)e(kt)$ for all $t \in \mathbb{R}$, where $g(0) = \gamma$, and the other Fourier coefficients satisfy the uniform bound

$$g(k) \ll \min\{|k|^{-1}, |k|^{-2}\Delta^{-1}\} \quad (k \neq 0). \tag{7}$$

From properties (i)–(iii) it follows that

$$F(x;d,c) = \sum_{\substack{n\le x\\ n\equiv c \,(\mathrm{mod}\, d)}} \Lambda(n)\Psi(\gamma n + \delta) + O\big(V(\mathcal{I},x)\log x\big), \tag{8}$$

where $V(\mathcal{I},x)$ is the number of positive integers $n \le x$ such that

$$\{\gamma n + \delta\} \in \mathcal{I} = [0,\Delta) \cup (\gamma - \Delta, \gamma + \Delta) \cup (1-\Delta, 1).$$

Since $|\mathcal{I}| = 4\Delta$, it follows from the definition (1) and Lemma 1 that

$$V(\mathcal{I},x) \ll \Delta x + x^{1-1/\tau+o(1)} \quad (x \to \infty). \tag{9}$$

Now let $K \ge \Delta^{-1}$ be a large real number, and let Ψ_K be the trigonometric polynomial defined by

$$\Psi_K(t) = \sum_{|k|\le K} g(k)e(kt). \tag{10}$$

From (7) it is clear that the estimate

$$\Psi(t) = \Psi_K(t) + O(K^{-1}\Delta^{-1}) \tag{11}$$

holds uniformly for all $t \in \mathbb{R}$. Combining (11) with (8) and taking into account (9), we derive that

$$F(x;d,c) = \sum_{\substack{n\le x\\ n\equiv c \,(\mathrm{mod}\, d)}} \Lambda(n)\Psi_K(\gamma n+\delta) + O(\Delta x\log x + x^{1-1/\tau+\varepsilon} + K^{-1}\Delta^{-1}x).$$

For fixed $A \in (0,1)$ (to be specified below) we now set

$$\Delta = x^{-A/2} \quad \text{and} \quad K = x^A.$$

By the definition (10) it follows that

$$F(x;d,c) = \sum_{|k|\le x^A} g(k)e(k\delta) \sum_{\substack{n\le x\\ n\equiv c \,(\mathrm{mod}\, d)}} \Lambda(n)e(k\gamma n) + O(x^{1-1/\tau+\varepsilon} + x^{1-A/2+\varepsilon}).$$

Using Lemma 4 together with (7) we see that

$$\sum_{\substack{|k|\le x^A\\ k\ne 0}} g(k)e(k\delta) \sum_{\substack{n\le x\\ n\equiv c\,(\mathrm{mod}\,d)}} \Lambda(n)e(k\gamma n) \ll \sum_{\substack{|k|\le x^A\\ k\ne 0}} |k|^{-1}\Big|\sum_{\substack{n\le x\\ n\equiv c\,(\mathrm{mod}\,d)}} \Lambda(n)e(k\gamma n)\Big| \ll x^{\frac{A+2+1/\tau}{2+2/\tau}+\varepsilon} + x^{4/5}(\log x)^4.$$

Since $g(0)=\gamma$ we therefore have

$$F(x;d,c) = \gamma \sum_{\substack{n\le x\\ n\equiv c\,(\mathrm{mod}\,d)}} \Lambda(n) + O\big(x^{\frac{A+2+1/\tau}{2+2/\tau}+\varepsilon} + x^{4/5+\varepsilon} + x^{1-1/\tau+\varepsilon} + x^{1-A/2+\varepsilon}\big).$$

Taking $A = 1/(2\tau+1)$ we obtain the desired estimate (6). ∎

4. Construction of Carmichael numbers. In this section, we outline our proof of Theorem 1. We shall be brief since our construction of Carmichael numbers composed of primes from the Beatty sequence $\mathscr{B}_{\alpha,\beta}$ closely parallels (and relies on) the construction of "ordinary" Carmichael numbers given in [1]. Here, we discuss only those modifications that are needed to establish Theorem 1.

Let $\mathscr{P}$ denote the set of all prime numbers, and set $\mathscr{P}_{\alpha,\beta} = \mathscr{P} \cap \mathscr{B}_{\alpha,\beta}$. The underlying idea behind our proof of Theorem 1 is to show that $\mathscr{P}_{\alpha,\beta}$ is sufficiently well-distributed over arithmetic progressions so that, following the method of [1], the primes used to form Carmichael numbers can all be drawn from $\mathscr{P}_{\alpha,\beta}$ rather than $\mathscr{P}$. Unfortunately, this idea appears only to succeed in the case that α is of finite type, which we now assume for the remainder of this section.

Let $\tau = \tau(\alpha) < \infty$ be the type of α. From the standard estimate

$$\sum_{n\le x} \Lambda(n) = \sum_{p\le x} \log p + O(x^{1/2})$$

together with Theorem 2, it follows that

$$\Big|\sum_{\substack{p\le x,\ p\in\mathscr{B}_{\alpha,\beta}\\ p\equiv c\,(\mathrm{mod}\,d)}} \log p - \frac{1}{\alpha}\sum_{\substack{p\le x\\ p\equiv c\,(\mathrm{mod}\,d)}} \log p\Big| \le x^{1-1/(4\tau+2)+\varepsilon} \quad (x \ge x_1(\alpha,\beta,\varepsilon)).$$

For any modulus $d \le (4\alpha)^{-1}x^{1/(4\tau+2)-\varepsilon}$ the right side of this inequality does not exceed $x/(4\alpha\varphi(d))$; therefore, applying [1, Theorem 2.1] and taking into account the above inequality, we derive the following statement, which plays a role in our construction analogous to that played by [1, Theorem 2.1].

LEMMA 5. *For every $B \in \big(0, \frac{1}{4\tau+2}\big)$ there exist numbers $\eta_B > 0$, $x_2(B)$ and D_B such that for all $x \ge x_2(B)$ there is a set $\mathcal{D}_B(x)$ consisting of at*

most D_B integers such that

$$\left| \sum_{\substack{p \le x,\ p \in \mathscr{B}_{\alpha,\beta} \\ p \equiv c \,(\mathrm{mod}\, d)}} \log p - \frac{x}{\alpha\varphi(d)} \right| \le \frac{x}{2\alpha\varphi(d)}$$

whenever d is not divisible by any element of $\mathcal{D}_B(x)$, $1 \le d \le x^B$, and c is coprime to d. Furthermore, every number in $\mathcal{D}_B(x)$ exceeds $\log x$, and all, but at most one, exceed x^{η_B}.

We remark that, in the statement of Lemma 5, η_B, $x_2(B)$, D_B and $\mathcal{D}_B(x)$ all depend on the parameters α and β, but we have suppressed this from the notation for the sake of clarity. Similarly, $x_3(B)$ depends on α and β in the statement of Lemma 6 below.

As an application of Lemma 5 we deduce the following statement, which extends [1, Theorem 3.1] to the setting of primes in a Beatty sequence.

LEMMA 6. *Suppose that $B \in \left(0, \frac{1}{4\tau+2}\right)$. There exists a number $x_3(B)$ such that if $x \ge x_3(B)$ and L is a squarefree integer not divisible by any prime exceeding $x^{(1-B)/2}$ and for which $\sum_{\text{prime } q|L} 1/q \le (1-B)/(32\alpha)$, then there is a positive integer $k \le x^{1-B}$ with $\gcd(k, L) = 1$ such that*

$$\#\{d \,|\, L : dk + 1 \le x \text{ and } p = dk + 1 \text{ is a prime in } \mathscr{B}_{\alpha,\beta}\} \ge \frac{2^{-D_B-2}}{\alpha \log x} \#\{d \,|\, L : 1 \le d \le x^B\}.$$

Sketch of proof. Let $\pi(x; d, a)$ [resp. $\pi_{\alpha,\beta}(x; d, a)$] be the number of primes [resp. primes in $\mathscr{P}_{\alpha,\beta}$] up to x that belong to the arithmetic progression a mod d. Using Lemma 5 we can replace the lower bound [1, Equation (3.2)] with the bound

$$\pi_{\alpha,\beta}(dx^{1-B}; d, 1) \ge \frac{1}{2\alpha} \frac{dx^{1-B}}{\varphi(d) \log x}.$$

Also, since $\pi_{\alpha,\beta}(x; d, a)$ never exceeds $\pi(x; d, a)$, the upper bound that follows [1, equation (3.2)] can be replaced with the bound

$$\pi_{\alpha,\beta}(dx^{1-B}; dq, 1) \le \frac{8}{q(1-B)} \frac{dx^{1-B}}{\varphi(d) \log x}.$$

Taking into account the inequality $\sum_{\text{prime } q|L} 1/q \le (1-B)/(32\alpha)$, the proof is completed using arguments given in the proof of [1, Theorem 3.1]. ∎

Let $\pi(x)$ be the number of primes $p \le x$, and let $\pi(x, y)$ be the number of those for which $p - 1$ is free of prime factors exceeding y. As in [1], we denote by $\mathcal{E}$ the set of numbers E in the range $0 < E < 1$ for which there exist numbers $x_4(E)$, $\gamma(E) > 0$ such that

$$\pi(x, x^{1-E}) \ge \gamma(E)\pi(x)$$

for all $x \ge x_4(E)$. With only a very slight modification to the proof of [1, Theorem 4.1], using Lemma 6 in place of [1, Theorem 3.1], we derive the following quantitative version of Theorem 1.

THEOREM 3. *For each $E \in \mathcal{E}$, $B \in \left(0, \frac{1}{4\tau+2}\right)$ and $\varepsilon > 0$, there is a number $x_4 = x_4(\alpha, \beta, E, B, \varepsilon)$ such that for any $x \ge x_4$, there are at least $x^{EB-\varepsilon}$ Carmichael numbers up to x composed solely of primes from $\mathscr{P}_{\alpha,\beta}$.*

Acknowledgements. The authors thank the referee for carefully reading the original manuscript and for several helpful comments and suggestions.

REFERENCES

[1] W. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. (2) 139 (1994), 703–722.

[2] A. Balog and A. Perelli, *Exponential sums over primes in an arithmetic progression*, Proc. Amer. Math. Soc. 93 (1985), 578–582.

[3] W. Banks, *Carmichael numbers with a square totient*, Canad. Math. Bull. 52 (2009), 3–8.

[4] —, *Carmichael numbers with a totient of the form $a^2 + nb^2$*, Monatsh. Math., to appear.

[5] W. Banks and C. Pomerance, *On Carmichael numbers in arithmetic progressions*, J. Austral. Math. Soc. 88 (2010), 313–321.

[6] W. Banks and I. Shparlinski, *Prime numbers with Beatty sequences*, Colloq. Math. 115 (2009), 147–157.

[7] Y. Bugeaud, *Approximation by Algebraic Numbers*, Cambridge Tracts in Math. 160, Cambridge Univ. Press, Cambridge, 2004.

[8] L. Dickson, *A new extension of Dirichlet's theorem on prime numbers*, Messenger of Math. 33 (1904), 155–161.

[9] J. Grantham, *There are infinitely many Perrin pseudoprimes*, J. Number Theory 130 (2010), 1117–1128.

[10] A. Khintchine [A. Khinchin], *Zur metrischen Theorie der diophantischen Approximationen*, Math. Z. 24 (1926), 706–714.

[11] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Pure Appl. Math., Wiley-Interscience, New York, 1974.

[12] A. Lavrik, *Analytic method of estimates of trigonometric sums by the primes of an arithmetic progression*, Dokl. Akad. Nauk SSSR 248 (1979), 1059–1063 (in Russian); English transl.: Soviet Math. Dokl. 20 (1979), 1121–1124.

[13] K. Roth, *Rational approximations to algebraic numbers*, Mathematika 2 (1955), 1–20.

[14] —, Corrigendum to [13], ibid. 2 (1955), 168.

[15] W. Schmidt, *Diophantine Approximation*, Lecture Notes in Math. 785, Springer, Berlin, 1980.

[16] I. Vinogradov, *The Method of Trigonometrical Sums in the Theory of Numbers*, Dover Publ., Mineola, NY, 2004.

William D. Banks, Aaron M. Yeager
Department of Mathematics
University of Missouri
Columbia, MO 65211, U.S.A.
E-mail: bankswd@missouri.edu
amydm6@mail.missouri.edu

Received 30 July 2011;
revised 25 October 2011 (5529)