CARMICHAEL MEETS CHEBOTAREV

WILLIAM D. BANKS, AHMET M. GÜLOĞLU, AND AARON M. YEAGER

Abstract. For any finite Galois extension K of $\mathbb{Q}$ and any conjugacy class C in $\mathrm{Gal}(K/\mathbb{Q})$, we show that there exist infinitely many Carmichael numbers composed solely of primes for which the associated class of Frobenius automorphisms is C. This result implies that for every natural number n there are infinitely many Carmichael numbers of the form $a^2 + nb^2$ with $a, b \in \mathbb{Z}$.

1. Introduction

For every prime number N, *Fermat's little theorem* asserts that

$$a^N \equiv a \ (\mathrm{mod}\ N) \qquad \text{for all } a \in \mathbb{Z}. \tag{1.1}$$

Around 1910, Carmichael began an in-depth study of *composite* numbers N with this property, which are now known as *Carmichael numbers.* In 1994 the existence of infinitely many Carmichael numbers was established by Alford, Granville and Pomerance [1]. The aim of the present work is to prove the following extension of their result.

Theorem 1.1. *Let $K/\mathbb{Q}$ be a finite Galois extension, and let C be a fixed conjugacy class in $\mathrm{Gal}(K/\mathbb{Q})$. Then, there are infinitely many Carmichael numbers which are composed solely of primes for which the associated class of Frobenius automorphisms is the class C.*

Let $K/\mathbb{Q}$ be an arbitrary number field and K_0 its Galois closure. Taking the conjugacy class of the identity automorphism of K_0 in Theorem 1.1, it follows that there exist infinitely many Carmichael numbers composed solely of primes that split completely in K_0. Since such primes must also split completely in K, we deduce the following statement, recovering a recent result of Grantham [8, Theorem 2.1] on the existence of infinitely many *Carmichael-Frobenius numbers* with respect to K.

Corollary 1.2. *For any fixed algebraic number field K, there are infinitely many Carmichael numbers which are composed solely of primes that split completely in K.*

As prime numbers and Carmichael numbers are linked by the common property (1.1), it is natural to ask whether certain questions about primes can also be settled for Carmichael numbers; see [2, 3, 6]. For example, it is well known that for every natural number n, there are infinitely many primes of the form $a^2 + nb^2$ with $a, b \in \mathbb{Z}$ (see the book [4] by Cox), and thus it is natural to ask whether the same result holds for the set of Carmichael numbers. In view of Corollary 1.2, we give an affirmative answer to this question.

1991 *Mathematics Subject Classification.* Primary 11N25, Secondary 11R45.

Key words and phrases. Carmichael numbers, Chebotarev density theorem.

Corollary 1.3. *For any fixed integer $n \geqslant 1$, there are infinitely many Carmichael numbers of the form $a^2 + nb^2$ with $a, b \in \mathbb{Z}$.*

To see why, let $S_n = \{a^2 + nb^2 \ : \ a, b \in \mathbb{Z}\}$, and let K_n be the ring class field associated to the order $\mathbb{Z}[\sqrt{-n}\,]$ in the imaginary quadratic field $\mathbb{Q}(\sqrt{-n}\,)$. According to [4, Theorem 9.4], if p is an odd prime not dividing n, then p splits completely in K_n if and only if $p \in S_n$. Applying Corollary 1.2 with $K = K_n$, we see that there are infinitely Carmichael numbers N composed solely of primes $p \in S_n$. Since S_n is closed under multiplication, every such N also lies in S_n, and the corollary follows.

In a different direction, taking $K = \mathbb{Q}(\mu_d)$, where μ_d is a primitive d-th root of unity, we recover the following result.

Corollary 1.4. *For any coprime integers a and $d \geqslant 1$, there are infinitely many Carmichael numbers composed solely of primes $p \equiv a \pmod{d}$.*

Matomäki [12] has recently shown that whenever $\gcd(a, m) = 1$ and a is a quadratic residue mod m, there are infinitely many Carmichael numbers in the progression a mod m. Assuming the necessary compability between the numbers a, m and the conjugacy class C in $\mathrm{Gal}(K/\mathbb{Q})$, it should be possible to combine the methods of [12] with those in our proof of Theorem 1.1 to show that there are infinitely many Carmichael numbers in the arithmetic progression a mod m which are composed solely of primes for which C is the associated class of Frobenius automorphisms. We thank the referee for posing this question and leave it as an open problem for the interested reader.

2. Preliminaries

Let $K/\mathbb{Q}$ be a finite Galois extension of degree $n_K = [K : \mathbb{Q}]$ and absolute discriminant $\mathscr{D}_K$. We put

$$\mathbb{N}_K = \big\{d \in \mathbb{N} \ : \ \gcd(d, \mathscr{D}_K) = 1\big\}. \tag{2.1}$$

For any Galois extension M/N and any unramified prime ideal $\mathfrak{p}$ of N, we denote by $(\mathfrak{p}, M|N)$ the conjugacy class of Frobenius automorphisms of $\mathrm{Gal}(M/N)$ corresponding to the prime ideals of M above $\mathfrak{p}$.

Given a conjugacy class C in $\mathrm{Gal}(K/\mathbb{Q})$, let

$$\mathscr{P}_C = \{p \in \mathbb{N}_K \ : \ p \text{ prime}, \ (p, K|\mathbb{Q}) = C\}.$$

For $d \in \mathbb{N}$ and M a number field, put $M_d = M(\mu_d)$, where μ_d is a primitive d-th root of unity. According to [15, Proposition 2.7], the discriminant of $\mathbb{Q}_d$ is

$$\mathscr{D}_{\mathbb{Q}_d} = (-1)^{\phi(d)/2} \frac{d^{\phi(d)}}{\prod_{p \mid d} p^{\phi(d)/(p-1)}}, \tag{2.2}$$

where $\phi(\cdot)$ is the Euler function.

Lemma 2.1. *For each $d \in \mathbb{N}_K$, K_d is a Galois extension of $\mathbb{Q}$ of degree $n_K\phi(d)$ with discriminant*

$$\mathscr{D}_{K_d} = \mathscr{D}_K^{\phi(d)} \mathscr{D}_{\mathbb{Q}_d}^{n_K}.$$

Furthermore, $\mathrm{Gal}(K_d/\mathbb{Q}) \simeq \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}_d/\mathbb{Q})$, *where the isomorphism is given by the restriction map $\sigma \to (\sigma_{|K}, \sigma_{|\mathbb{Q}_d})$.*

Proof. In view of (2.1) and (2.2), the discriminants $\mathscr{D}_K$ and $\mathscr{D}_{\mathbb{Q}_d}$ are coprime for every $d \in \mathbb{N}_K$. Put $L = K \cap \mathbb{Q}_d$. By [13, Ch.3, Corollary 2.10] the absolute discriminant $\mathscr{D}_L$ of L divides both $\mathscr{D}_K$ and $\mathscr{D}_{\mathbb{Q}_d}$; thus, $\mathscr{D}_L = 1$ and $K \cap \mathbb{Q}_d = L = \mathbb{Q}$. The result now follows from [13, Ch.1, Proposition 2.11], [5, 14.4, Proposition 21] and [5, 14.4, Corollary 22]. □

The constants $c_0, c_1, c_2, \ldots$ that appear in our proofs are assumed to be positive and depend only on the field K. All constants implied by the symbols O, $\ll$ and $\gg$ are absolute; we write O_K, $\ll_K$ and $\gg_K$ to indicate that the implied constant depends on K.

3. Zeros of Dedekind zeta functions

For each $d \in \mathbb{N}_K$, let $\zeta_d(s)$ be the Dedekind zeta function $\zeta_{K_d}(s)$ associated with the field K_d considered in §2.

Lemma 3.1. *There are constants $c_1, c_2 > 0$ depending only on K with the property that for all $T \geqslant 1$ and $U \geqslant 2$ there exists a proper integral ideal $\mathfrak{f} = \mathfrak{f}(K, U, T)$ of K such that for any $d \in \mathbb{N}_K$ with $d \leqslant U$, $\mathfrak{f} \mid d\mathcal{O}_K$, where $\mathcal{O}_K$ is the ring of integers of K, whenever $\zeta_d(s)$ has a zero $\beta + i\gamma$ in the region*

$$\Omega(T, U) = \left\{ \beta + i\gamma \ : \ \beta \geqslant 1 - \frac{c_1}{\log(c_2 TU)}, \ |\gamma| \leqslant T \right\}. \tag{3.1}$$

Proof. We use the notation of [16, §1]. For each $d \in \mathbb{N}_K$ with $d \leqslant U$, and any Dirichlet character χ modulo $(d) = d\mathcal{O}_K$ of conductor $\mathfrak{f}_\chi$, we see that

$$d_\chi := |\mathscr{D}_K| \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{f}_\chi) \underset{K}{\ll} d^{n_K} \leqslant U^{n_K},$$

Hence, it follows that $d_\chi \leqslant (c_2 U)^{n_K}$ for some constant $c_2 = c_2(K)$. Applying [16, Theorem 1.9] with $Q = (c_2 U)^{n_K}$ and

$$\mathscr{L} = \log(QT^{n_K}) = n_K \log(c_2 TU),$$

we see that for some constant $c_1 = c_1(K)$, any Hecke L-function $L(s, \chi)$ with $d_\chi \leqslant Q$ has at most one zero in the region $\Omega(T, U)$. Moreover, the remark following [16, Theorem 1.9] asserts that there is at most one function $L(s, \chi_*)$ vanishing in $\Omega(T, U)$ among all $L(s, \chi)$ associated with *primitive* characters χ with $d_\chi \leqslant Q$. If such a zero exists, then it is a real number β_* (which can be bounded in terms of Q). For such a zero we have

$$\beta_* \geqslant 1 - \frac{c_1}{\log(c_2 TU)} \geqslant 1 - \frac{c_1}{\log c_2}.$$

Replacing c_1 by a smaller constant (which also depends only on K), we can assume that $\zeta_K(\beta_*) \neq 0$, i.e., χ_* is not the trivial character.

By [13, Ch.7, Corollary 10.5]

$$\zeta_d(s) = \zeta_K(s) \prod_{\chi \neq 1} L(s, \chi, K_d|K)$$

is the product of Artin L-functions, where χ runs over the irreducible characters of $\mathrm{Gal}(K_d/K)$. Let K_χ be the fixed field of the kernel of χ. Then, χ is injective as a character of $\mathrm{Gal}(K_\chi/K)$. Hence, by [13, Ch.7, Theorem 10.6] there exists a *primitive* Dirichlet character $\widetilde{\chi}$ modulo the conductor $\mathfrak{f}_\chi$ of the extension K_χ/K such that

$$L(s, \chi, K_d|K) = L(s, \widetilde{\chi}).$$

Furthermore, since $K \subseteq K_\chi \subseteq K_d$, we see by [9, 5.1.5] and the last paragraph of [9, §6] that the conductor $\mathfrak{f}_\chi$ divides (d); thus, $d_{\widetilde{\chi}} \leqslant Q$.

Using the remarks above we conclude that $\zeta_d(s)$ vanishes in $\Omega(T, U)$ if and only if $L(s, \chi_*)$ is a factor of $\zeta_d(s)$ and $L(\beta_*, \chi_*) = 0$. In this case, we know that $\mathfrak{f}_{\chi_*} \mid (d)$ and $\mathfrak{f}_{\chi_*} \neq 1$; thus, we can take $\mathfrak{f} = \mathfrak{f}_{\chi_*}$. □

Lemma 3.2. *There are constants $c_3, c_4, c_5 > 0$ depending only on K with the property that for all $d \in \mathbb{N}_K$, $T \geqslant c_3 d$, and $\sigma \geqslant 1 - 1/c_5$, the number $N_d(\sigma, T)$ of zeros $\beta + i\gamma$ of $\zeta_d(s)$ with $\beta \geqslant \sigma$ and $|\gamma| \leqslant T$ satisfies the bound*

$$N_d(\sigma, T) \leqslant c_4 (Td)^{c_5(1-\sigma)}.$$

Proof. We continue to use notation of [16, §1]. As in the proof of Lemma 3.1, for each $d \in \mathbb{N}_K$ let H (in the notation of [16, §1]) denote the trivial subgroup of the ideal class group $I((d))/P_{(d)}$ modulo (d), and note that the quantities h_H and $d(H)$ defined by [16, Equation (1.1b)] satisfy the bound

$$\max\{h_H, d(H)\} \leqslant (cd)^{n_K}$$

for some constant $c = c(K)$ in view of [16, Lemma 1.16]. The result now follows by applying [16, Corollary 4.4] with $Q = (cd)^{n_K}$ and $T \geqslant c_3 d$, where $c_3 = c_3(K)$ is any constant that is large enough so that the conditions $T \gg 1$ and $T \geqslant n_K^2 h_H^{1/n_K}$ of [16, Corollary 4.4] are met (for the latter condition, any number $c_3 \geqslant c n_K^2$ suffices by the inequality above). □

4. Chebotarev Density Theorem

Our goal in this section is to provide a lower bound for the counting function of the set

$$\mathscr{P}_{C_d} = \big\{ p \in \mathscr{P}_C : \ p \equiv 1 \pmod d \big\}$$

using an effective version of the Chebotarev density theorem given by [10].

By [13, Ch.1, Corollary 10.4] we see that $p \equiv 1 \pmod d$ if and only if p splits completely in $\mathbb{Q}_d$ if and only if $(p, \mathbb{Q}_d|\mathbb{Q}) = \{\mathbf{1}_d\}$ for $p \in \mathbb{N}_K$, where $\mathbf{1}_d$ denotes the identity element of $\mathrm{Gal}(\mathbb{Q}_d|\mathbb{Q})$. It follows by the isomorphism in Lemma 2.1 that there exists a conjugacy class C_d in $\mathrm{Gal}(K_d/\mathbb{Q})$ (one that corresponds to $C \times \{\mathbf{1}_d\}$) with the property that

$$p \in \mathscr{P}_{C_d} \quad \Longleftrightarrow \quad (p, K_d|\mathbb{Q}) = C_d \quad (p \in \mathbb{N}_K).$$

Accordingly, we study the function

$$\pi_C(x; d, 1) = \#\{p \leqslant x \ : \ p \in \mathbb{N}_K, \, (p, K_d|\mathbb{Q}) = C_d\}$$

and its weighted version

$$\psi_C(x; d, 1) = \sum_{\substack{p, m: \ p^m \leqslant x \\ (p^m, K_d|\mathbb{Q}) = C_d}} \log p,$$

where the sum is taken over primes in $\mathbb{N}_K$. Our main result is the following:

Theorem 4.1. *There are constants $x_1, B > 0$ depending only on K with the property that for all $x \geqslant x_1$ and every $d \in \mathbb{N}_K$ with $d \leqslant x^B$,*

$$\pi_C(y; d, 1) \geqslant \frac{|C|}{2 n_K \phi(d)} \frac{y}{\log y} \qquad (x^{4/5} \leqslant y \leqslant x) \tag{4.1}$$

whenever $\zeta_d(s)$ has no zeros in the region

$$\Omega_B(x)=\left\{\beta+i\gamma\ :\ \beta\geqslant 1-\frac{c_1}{\log(c_2x^{4B})},\ |\gamma|\leqslant x^{3B}\right\}. \tag{4.2}$$

Proof. Let $B=B(K)$ be a constant in the interval $(0,\frac{1}{100})$ to be further determined below. For convenience, we set

$$\theta_B(y)=\frac{c_1\log y}{\log(c_2y^{5B})}. \tag{4.3}$$

For $x^{4/5}\leqslant y\leqslant x$, we have

$$1-\frac{\theta_B(y)}{\log y}\geqslant 1-\frac{c_1}{\log(c_2x^{4B})}\qquad\text{and}\qquad y^{3B}\leqslant x^{3B},$$

hence the region

$$\widetilde{\Omega}_B(y)=\left\{\beta+i\gamma\ :\ \beta\geqslant 1-\frac{\theta_B(y)}{\log y},\ |\gamma|\leqslant y^{3B}\right\}$$

is contained in $\Omega_B(x)$; therefore, $\zeta_d(s)$ has no zeros in $\widetilde{\Omega}_B(y)$ whenever it has no zeros in $\Omega_B(x)$.

Let g be a fixed element of C_d with $d\in\mathbb{N}_K$ and $d\leqslant x^B$, $H=\langle g\rangle$ the cyclic subgroup of G generated by g, E the fixed field of H, and $\widehat{H}$ the dual of H, i.e., the set of irreducible characters $\chi:H\to\mathbb{C}^\times$.

Applying [10, Theorem 7.1] with the choices $G=\mathrm{Gal}(K_d|\mathbb{Q})$ and $T=y^{3B}$, and taking into account the bounds

$$\begin{aligned}&|G|=n_{K_d}=\phi(d)n_K\ll_K d\leqslant y^{2B}\\&\log|\mathscr{D}_{K_d}|\ll\phi(d)\left(\log|\mathscr{D}_K|+n_K\log d\right)\ll_K y^{2B}\log y,\end{aligned} \tag{4.4}$$

which hold by Lemma 2.1 for all $d\leqslant x^B\leqslant y^{5B/4}$, we derive that

$$\psi_C(y;d,1)-\frac{|C|}{|G|}\,y+\frac{|C|}{|G|}\,Z_B(y)\ll_K\frac{|C|}{|G|}y^{1-B}\log y \tag{4.5}$$

where we have used $|C_d|=|C|$, and

$$Z_B(y)=\sum_{\chi\in\widehat{H}}\overline{\chi}(g)\Bigg(\sum_{\substack{\rho\\|\gamma|\leqslant T}}\frac{y^\rho}{\rho}-\sum_{\substack{\rho\\|\rho|<\frac{1}{2}}}\frac{1}{\rho}\Bigg).$$

Here, the inner sums are taken over the nontrivial zeros $\rho=\beta+i\gamma$ of the Artin L-functions $L(s,\chi,K_d|E)$ so that

$$\zeta_d(s)=\prod_{\chi\in\widehat{H}}L(s,\chi,K_d|E).$$

Assuming $\zeta_d(s)$ has no zeros in the region $\Omega_B(x)$, it follows by the functional equation of $\zeta_d(s)$ that every zero $\rho=\beta+i\gamma$ of $\zeta_d(s)$, and thus also of each $L(s,\chi,K_d|E)$, lies outside of the region

$$\left\{\beta+i\gamma\ :\ 0\leqslant\beta\leqslant\frac{\theta_B(y)}{\log y},\ |\gamma|\leqslant y^{3B}\right\},$$

and thus $|\rho| > \theta_B(y)/\log y \underset{K}{\gg} 1/\log y$ for every such zero. We conclude that

$$\sum_{\substack{\rho:\ \beta<\frac{1}{2}\\ |\gamma|\leqslant 1}} \frac{y^\rho}{\rho} - \sum_{\substack{\rho\\ |\rho|<\frac{1}{2}}} \frac{1}{\rho} \ll y^{1/2} \sum_{\substack{\rho\\ |\gamma|\leqslant 1}} \frac{1}{|\rho|} \underset{K}{\ll} n_\chi(0)\, y^{1/2}\log y,$$

where $n_\chi(t)$ is the number of zeros $\beta+i\gamma$ of $L(s,\chi,K_d|E)$ such that $0<\beta<1$ and $|\gamma-t|\leqslant 1$. By [10, Lemma 5.4],

$$n_\chi(t) \ll \log d_\chi + \frac{n_K\phi(d)}{|H|}\log(|t|+2), \tag{4.6}$$

where $d_\chi = |\mathscr{D}_E|\mathrm{N}_{E/\mathbb{Q}}(\mathfrak{f}_\chi)$. Summing over all characters $\chi\in\widehat{H}$ and using (4.6) we see that

$$\begin{aligned}\sum_{\chi\in\widehat{H}} \overline{\chi}(g)\Bigg(\sum_{\substack{\rho:\ \beta<\frac{1}{2}\\ |\gamma|\leqslant 1}} \frac{y^\rho}{\rho} - \sum_{\substack{\rho\\ |\rho|<\frac{1}{2}}} \frac{1}{\rho}\Bigg) &\underset{K}{\ll} y^{1/2}\log y \sum_{\chi\in\widehat{H}}\Bigg(\log d_\chi + \frac{d}{|H|}\Bigg)\\ &= y^{1/2}\log y\left(\log|\mathscr{D}_{K_d}| + y^{2B}\right) \underset{K}{\ll} y^{1/2+2B}\log^2 y,\end{aligned} \tag{4.7}$$

where the equaliy $|\mathscr{D}_{K_d}| = \prod_\chi d_\chi$ follows from [13, Ch.3, Corollary 2.10] and the Conductor-Discriminant formula [13, Ch.7, Proposition 11.9]. Moreover,

$$\sum_{\substack{\rho:\ \beta<\frac{1}{2}\\ 1<|\gamma|\leqslant y^{3B}}} \frac{y^\rho}{\rho} \ll y^{1/2} \sum_{\substack{\rho\\ 1\leqslant|\gamma|\leqslant y^{3B}}} \frac{1}{|\rho|} \leqslant y^{1/2} \sum_{j=1}^{\lfloor y^{3B}\rfloor} \sum_{\substack{\rho\\ j\leqslant|\gamma|\leqslant j+1}} \frac{1}{|\rho|};$$

thus, summing over the characters we obtain

$$\begin{aligned}\sum_{\chi\in\widehat{H}} \overline{\chi}(g) \sum_{\substack{\rho:\ \beta<\frac{1}{2}\\ 1<|\gamma|\leqslant y^{3B}}} \frac{y^\rho}{\rho} &\ll y^{1/2} \sum_{j=1}^{\lfloor y^{3B}\rfloor} \frac{1}{j} \sum_{\chi\in\widehat{H}}\Bigg(\log d_\chi + \frac{n_K\phi(d)}{|H|}\log(j+1)\Bigg)\\ &\underset{K}{\ll} y^{1/2+2B}\log^2 y.\end{aligned} \tag{4.8}$$

In view of (4.7) and (4.8) we have

$$Z_B(y) = \sum_{\chi\in\widehat{H}} \overline{\chi}(g) \sum_{\substack{\rho:\ \beta\geqslant\frac{1}{2}\\ |\gamma|\leqslant y^{3B}}} \frac{y^\rho}{\rho} + O_K\big(y^{1/2+2B}\log^2 y\big). \tag{4.9}$$

To estimate the sum in (4.9), we use ideas (and notation) from the proof of [1, Theorem 2.1]. For each zero $\rho=\beta+i\gamma$ in the sum, we have $|y^\rho| = y^\beta$ and $|\rho|\geqslant \frac{1}{4}+|\gamma| \gg 1+|\gamma|$. Fix $\chi\in\widehat{H}$ and write $\sum_\sigma^\alpha$ for any sum over all zeros $\beta+i\gamma$ of $L(s,\chi,K_d/E)$ with $\sigma\leqslant\beta<\alpha$ and $|\gamma|\leqslant y^{3B}$. Put $\tau = 1-\theta_B(y)/\log y$, and note that

$$\sum_\tau^1 \frac{y^\rho}{\rho} = 0$$

since $\zeta_d(s)$ has no zeros in $\widetilde{\Omega}_B(y)$. Hence, using the upper bound $y^\beta \leqslant y^{1-1/c_5}$ when $\beta\leqslant 1-1/c_5$ and the identity $y^\beta = y^{1-1/c_5} + \log y\int_{1-1/c_5}^\beta y^\sigma\,d\sigma$ when β lies in the range $1-1/c_5 \leqslant \beta \leqslant \tau$, it follows that

$$\begin{aligned}
\sum_{\substack{\rho\\ \beta\geqslant\frac{1}{2},\ |\gamma|\leqslant y^{3B}}} \frac{y^\rho}{\rho} &= \sum_{1/2}^{1-1/c_5}\frac{y^\rho}{\rho} + \sum_{1-1/c_5}^{\tau}\frac{y^\rho}{\rho} \ll \sum_{1/2}^{1-1/c_5}\frac{y^\beta}{1+|\gamma|} + \sum_{1-1/c_5}^{\tau}\frac{y^\beta}{1+|\gamma|}\\
&\ll y^{1-1/c_5}\sum_{1/2}^{\tau}\frac{1}{1+|\gamma|} + \log y\sum_{1-1/c_5}^{\tau}\frac{1}{1+|\gamma|}\int_{1-1/c_5}^{\beta} y^\sigma\,d\sigma \qquad (4.10)\\
&\ll y^{1-1/c_5}\sum_{\substack{\rho\\ |\gamma|\leqslant y^{3B}}}\frac{1}{1+|\gamma|} + \log y\int_{1-1/c_5}^{\tau} y^\sigma\left(\sum_{\sigma}^{\tau}\frac{1}{1+|\gamma|}\right)d\sigma.
\end{aligned}$$

Summing over all characters and using (4.6) the first term above can be bounded as before:

$$\begin{aligned}
\sum_{\chi\in\widehat{H}}\overline{\chi}(g)\sum_{\substack{\rho\\ |\gamma|\leqslant y^{3B}}}\frac{1}{1+|\gamma|} &\leqslant \sum_{\chi\in\widehat{H}}\sum_{j=0}^{\lfloor y^{3B}\rfloor}\sum_{\substack{\rho\\ j\leqslant|\gamma|\leqslant j+1}}\frac{1}{1+|\gamma|} \qquad (4.11)\\
&\ll_K \sum_{j=0}^{\lfloor y^{3B}\rfloor}\frac{d\log d + d\log(1+j)}{j+1} \ll y^{2B}\log^2 y.
\end{aligned}$$

Let $N_\chi(\sigma,T)$ be the number of zeros $\beta+i\gamma$ of $L(s,\chi,K_d|E)$ with $\beta\geqslant\sigma$ and $|\gamma|\leqslant T$. Then, it follows by partial summation that for $\sigma\geqslant 1-1/c_5$,

$$\sum_{\sigma}^{\tau}\frac{1}{1+|\gamma|} \leqslant N_\chi(\sigma,c_3d) + \frac{N_\chi(\sigma,y^{3B})}{y^{3B}} + \int_{c_3d}^{y^{3B}}\frac{N_\chi(\sigma,t)}{t^2}\,dt$$

Summing over all characters χ once again we obtain

$$\sum_{\chi\in\widehat{H}}\overline{\chi}(g)\sum_{\sigma}^{\tau}\frac{1}{1+|\gamma|} \ll N_d(\sigma,c_3d) + \frac{N_d(\sigma,y^{3B})}{y^{3B}} + \int_{c_3d}^{y^{3B}}\frac{N_d(\sigma,t)}{t^2}\,dt \tag{4.12}$$

By Lemma 3.2, we have for all $\sigma\geqslant 1-1/c_5$ and $d\leqslant x^B\leqslant y^{2B}$,

$$\begin{aligned}
\sum_{\chi\in\widehat{H}}\overline{\chi}(g)\sum_{\sigma}^{\tau}\frac{1}{1+|\gamma|} &\ll c_4(c_3d^2)^{c_5(1-\sigma)} + \frac{c_4(y^{3B}d)^{c_5(1-\sigma)}}{y^{3B}} + \int_{c_3d}^{y^{3B}}\frac{c_4(td)^{c_5(1-\sigma)}}{t^2}\,dt\\
&\ll_K y^{4c_5B(1-\sigma)} + y^{2c_5B(1-\sigma)}\int_1^{y^{3B}}\frac{t^{c_5(1-\sigma)}}{t^2}\,dt.
\end{aligned}$$

Using the bound

$$\int_1^{y^{3B}}\frac{t^{c_5(1-\sigma)}}{t^2}\,dt \ll_K \begin{cases}\log y & \text{if } 1-1/c_5\leqslant\sigma\leqslant 1-1/(2c_5)\\ 1 & \text{if } \sigma\geqslant 1-1/(2c_5),\end{cases}$$

and assuming that $B < 1/(4c_5)$, we derive that

$$\begin{aligned}
&\int_{1-1/c_5}^{\tau} y^{\sigma}\Bigg(\sum_{\chi\in\widehat{H}} \overline{\chi}(g) \sum_{\sigma}^{\tau} \frac{1}{1+|\gamma|}\Bigg)\,d\sigma\\
&\qquad \underset{K}{\ll} \int_{1-1/c_5}^{\tau} y^{\sigma}\cdot y^{4c_5B(1-\sigma)}\,d\sigma + \int_{1-1/c_5}^{1-1/(2c_5)} y^{\sigma}\cdot y^{2c_5B(1-\sigma)}\log y\,d\sigma\\
&\qquad = y^{4c_5B}\int_{1-1/c_5}^{\tau} y^{\sigma(1-4c_5B)}\,d\sigma + y^{2c_5B}\log y\int_{1-1/c_5}^{1-1/(2c_5)} y^{\sigma(1-2c_5B)}\,d\sigma\\
&\qquad \ll y^{4c_5B}\,\frac{y^{\tau(1-4c_5B)}}{(1-4c_5B)\log y} + y^{2c_5B}\,\frac{y^{(1-1/(2c_5))(1-2c_5B)}}{(1-2c_5B)}\\
&\qquad = \frac{y\,\exp(-(1-4c_5B)\theta_B(y))}{(1-4c_5B)\log y} + \frac{y^{1+B-1/(2c_5)}}{(1-2c_5B)},
\end{aligned}$$

where we have used the definition of τ in the last step. Combining this bound with (4.9), (4.10) and (4.11), and assuming further that $B \leqslant 1/(5c_5)$, we find that

$$Z_B(y) \underset{K}{\ll} y\,\exp(-\tfrac{1}{5}\theta_B(y)).$$

Finally, using (4.5) we see that

$$\left|\psi_C(y;d,1) - \frac{|C|}{|G|}\,y\right| \leqslant \frac{|C|}{|G|}\,cy\left(\exp(-\tfrac{1}{5}\theta_B(y)) + y^{-B}\log^2 y\right) \tag{4.13}$$

for some sufficiently large constant $c = c(K)$.

To finish the proof, we now put

$$B = \min\left\{\frac{1}{100}, \frac{1}{5c_5}, \frac{c_1}{30\log(6c)}\right\}.$$

Note that B depends only on K, the bound (4.13) holds, and we have

$$c\,\exp\left(-\frac{c_1}{30\,B}\right) \leqslant \frac{1}{6}.$$

On the other hand, from the definition (4.3) one sees that $\theta_B(y) \geqslant c_1/(6B)$ holds for any $y \geqslant y_1$, where $y_1 = \exp((\log c_2)/B)$. Therefore,

$$c\,\exp(-\tfrac{1}{5}\theta_B(y)) \leqslant \frac{1}{6} \qquad (y \geqslant y_1). \tag{4.14}$$

Increasing the value of y_1 if necessary, we also have

$$c\,y^{-B}\log^2 y \leqslant \frac{1}{6} \qquad (y \geqslant y_1). \tag{4.15}$$

Put $x_1 = y_1^{5/4}$ so that the condition $y \geqslant y_1$ is satisfied whenever $x^{4/5} \leqslant y \leqslant x$ and $x \geqslant x_1$. Combining the bounds (4.13), (4.14) and (4.15) we obtain

$$\psi_C(y;d,1) \geqslant \frac{2|C|}{3|G|}\,y \qquad (x^{4/5} \leqslant y \leqslant x) \tag{4.16}$$

for all $x \geqslant x_1$. Partial summation yields

$$\pi_C(y;d,1) \geqslant \frac{2|C|}{3|G|}\,\frac{y}{\log y} - \frac{4\sqrt{y}}{\log y} \geqslant \frac{|C|}{2|G|}\,\frac{y}{\log y} \qquad (x^{4/5} \leqslant y \leqslant x), \tag{4.17}$$

where the last inequality holds when $\sqrt{y} \geqslant 24|G|/|C|$, which is guaranteed by our choice of B and d with $d \leqslant x^B$. We finish the proof by noting that $|G| = n_K\phi(d)$. □

5. Construction of Carmichael numbers

In view of Theorem 4.1, our construction of Carmichael numbers with the property stated in Theorem 1.1 follows closely that given in [1]. We shall be brief, since most of the details are the same. Our principal tool is the following variant of [1, Theorem 3.1]:

Lemma 5.1. *Let the constants x_1, B have the property stated in Theorem 4.1, and suppose that $x \geqslant x_1$. If L is any squarefree number in $\mathbb{N}_K$ that is not divisible by any prime exceeding $x^{(1-B)/2}$, and*

$$\sum_{\text{prime } q \mid L} \frac{1}{q} \leqslant \frac{1}{60n_K},$$

then there is a positive number $k \leqslant x^{1-B}$ with $\gcd(k, L) = 1$ such that

$$\#\big\{d \mid L \ : \ dk+1 \in \mathscr{P}_C,\ dk+1 \leqslant x\big\} \geqslant \frac{1}{6n_K \log x} \cdot \#\big\{d \mid L \ : \ d \leqslant x^B\big\}.$$

Proof. We use ideas (and notation) from the proof of [1, Theorem 3.1].

Observe that the region $\Omega_B(x)$ defined by (4.2) is the same as the region $\Omega(T, U)$ defined by (3.1) when we put $T = x^{3B}$ and $U = x^B$.

Fix a prime p_0 with the property that $p_0 \mid \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{f})$, where $\mathfrak{f} = \mathfrak{f}(K, x^B, x^{3B})$ is given by Lemma 3.1. If L is divisible by p_0 let $L' = L/p_0$; otherwise, let $L' = L$. Note that

$$\#\big\{d \mid L' \ : \ d \leqslant y\big\} \geqslant \frac{1}{2} \cdot \#\big\{d \mid L \ : \ d \leqslant y\big\} \qquad (y \geqslant 1) \tag{5.1}$$

(see [1, p. 716]). Since $p_0 \nmid L'$, for every divisor d of L' with $d \leqslant x^B$, Lemma 3.1 shows that $\zeta_d(s)$ has no zeros in $\Omega_B(x)$; therefore, using the lower bound (4.1) from Theorem 4.1 we have

$$\pi_C(dx^{1-B}; d, 1) \geqslant \frac{|C|}{2n_K} \frac{dx^{1-B}}{\phi(d) \log x}.$$

On the other hand, since any prime divisor q of L does not exceed $x^{(1-B)/2}$, we have from [11, Theorem 2]:

$$\pi_C(dx^{1-B}; dq, 1) \leqslant \pi(dx^{1-B}; dq, 1) \leqslant \frac{10}{q} \frac{dx^{1-B}}{\phi(d) \log x}.$$

Therefore, the number of primes $p \in \mathscr{P}_{C_d}$ with $p \leqslant dx^{1-B}$ and $\gcd((p-1)/d, L) = 1$ is at least

$$\begin{aligned} &\pi_C(dx^{1-B}; d, 1) - \sum_{\text{prime } q \mid L} \pi_C(dx^{1-B}; dq, 1) \\ &\qquad \geqslant \left(\frac{1}{2n_K} - 10 \sum_{\text{prime } q \mid L} \frac{1}{q}\right) \frac{dx^{1-B}}{\phi(d) \log x} \geqslant \frac{x^{1-B}}{3n_K \log x}. \end{aligned}$$

Using this bound together with (5.1) (instead of [1, Equation (3.1)]), the proof can be concluded in the same manner as that of [1, Theorem 3.1]; the remaining details are omitted. □

We are now in a position to establish a quantitative version of Theorem 1.1.

Theorem 5.2. *There are constants* $x_0, c_0 > 0$ *depending only on* K *such that for all* $x \geqslant x_0$*, there are at least* x^{c_0} *Carmichael numbers up to* x *that are composed solely of primes which split completely in* K*.*

Proof. To prove this, we only need to modify the proof of [1, Theorem 4.1] slightly, as follows.

Let $\mathcal{E}$ be the set of numbers $E \in (0,1)$ for which there exists a constant $x_2 > 0$ depending only on E such that

$$\pi(x, x^{1-E}) \underset{E}{\gg} \pi(x) \qquad (x \geqslant x_2), \tag{5.2}$$

where $\pi(x,y)$ denotes the number of primes $p \leqslant x$ such that $p-1$ is free of prime factors exceeding y.

Fix $E = 3/5$, which lies in the set $\mathcal{E}$ (see, e.g., [7]), and let x_2 be a number for which the bound (5.2) holds. Let x_1, B be numbers with the property stated in Theorem 4.1, and put $x_3 = \max\{x_1, x_2\}$. Note that our choice of x_3 depends only on K.

Let $y \geqslant 2$ be a parameter and Q the set of primes $q \in \mathbb{N}_K$ with

$$y^{5/2}/\log y < q \leqslant y^{5/2}$$

for which $q-1$ is free of prime factors exceeding y. By (5.2)

$$|Q| \geqslant \pi(y^{5/2}, y) - \pi(y^{5/2}/\log y) - \sum_{q \mid \mathscr{D}_K} 1 \gg y^{5/2}/\log y \tag{5.3}$$

for all sufficiently large y. Let L be the product of primes in Q; then

$$\log L = \sum_{q \in Q} \log q \leqslant \sum_{q \leqslant y^{5/2}} \log q = \vartheta(y^{5/2}) \leqslant 1.1 y^{5/2}$$

for all $y > 0$, where we have used [14] for the last inequality. Furthermore,

$$\lambda(L) = \prod_{p^a \,\|\, \lambda(L)} p^a \leqslant \prod_{p \leqslant y} p^{\lfloor \frac{\log y^{5/2}}{\log p} \rfloor} \leqslant y^{5\pi(y)/2} \leqslant e^{\pi \cdot y} \tag{5.4}$$

where the last inequality follows again by [14]. We also have

$$n(G_L) \leqslant \lambda(L)(1 + \log L) \leqslant e^{\pi y}(1 + 1.1 y^{5/2}) \leqslant e^{5y}, \tag{5.5}$$

where $G_L = (\mathbb{Z}/L\mathbb{Z})^*$.

Let $x = e^{y^{1+\delta}}$ where $\delta = 5\varepsilon/(8B)$. Since

$$\sum_{\text{prime } q \mid L} \frac{1}{q} \leqslant \sum_{y^{5/2}/\log y < q \leqslant y^{5/2}} \frac{1}{q} \leqslant 4 \frac{\log\log y}{5 \log y} \leqslant \frac{1}{60 n_K}$$

for sufficiently large y, it follows from Lemma 5.1 that there exists an integer k coprime to L, for which the set $\mathcal{P}$ of primes $p \leqslant x$ with $p \in \mathscr{P}_C$ and $p = dk + 1$ for some divisor d of L, satisfies

$$|\mathcal{P}| \geqslant \frac{1}{6 n_K \log x} \cdot \#\big\{d \mid L \ : \ 1 \leqslant d \leqslant x^B\big\}. \tag{5.6}$$

The product of any

$$u := \left[\frac{\log(x^B)}{\log y^{5/2}}\right]$$

distinct prime factors of L, is a divisor d of L with $d \leqslant x^B$. We deduce from (5.3) that

$$\begin{aligned} \#\{d|L : 1 \leqslant d \leqslant x^B\} &\geqslant \binom{\omega(L)}{u} \geqslant \left(\frac{\omega(L)}{u}\right)^u \\ &\geqslant \left(\frac{cy^{5/2}}{2B\log x}\right)^u \end{aligned} \tag{5.7}$$

Thus, by (5.6) and the identity $(5/2 - 1 - \delta)2B/5 = 3B/5 - \varepsilon/4$,

$$|\mathcal{P}| \geqslant \frac{1}{6n_K \log x}\left(\frac{c}{2B}y^{5/2-1-\delta}\right)^{\lfloor \frac{2B\log x}{5\log y}\rfloor} \geqslant x^{3B/5-\varepsilon/3}$$

for all sufficiently large values of y. Now take $\mathcal{P}' = \mathcal{P}\backslash Q$. Since $|Q| \leqslant y^{5/2}$, it follows by the above inequality that

$$|\mathcal{P}'| \geqslant x^{3B/5-\varepsilon/2} \tag{5.8}$$

for all sufficiently large values of y.

We may view $\mathcal{P}'$ as a subset of the group $(\mathbb{Z}/L\mathbb{Z})^\star$ by considering the residue class of each $p \in \mathcal{P}'$ modulo L. If S is a subset of $\mathcal{P}'$ that contains more than one element and if

$$\Pi(S) := \prod_{p\in S} p \equiv 1 \pmod{L},$$

then $\Pi(S)$ is a Carmichael number. Indeed, every member of $\mathcal{P}'$ is 1 mod k so that $\Pi(S) \equiv 1 \pmod{k}$, and thus $\Pi(S) \equiv 1 \pmod{kL}$, since $(k, L) = 1$. However, if $p \in \mathcal{P}'$ then $p \in \mathcal{P}$ so that $p-1$ divides kL. Thus $\Pi(S)$ satisfies Korselt's criterion.

Let $t = e^{y^{1+\delta/2}}$. Then, by [1, Proposition 1.2], we see that the number of Carmichael numbers of the form $\Pi(S)$, where $S \subseteq \mathcal{P}'$ and $|S| \leqslant t$, is at least

$$\binom{|\mathcal{P}'|}{\lfloor t\rfloor}\binom{|\mathcal{P}'|}{n(G_L)}^{-1} \geqslant \left(\frac{|\mathcal{P}'|}{\lfloor t\rfloor}\right)^{\lfloor t\rfloor}|\mathcal{P}'|^{-n(G_L)} \geqslant x^{t(3B/5-\varepsilon)}$$

for all sufficiently large values of y, using (5.5) and (5.8). But each such Carmichael number $\Pi(S)$ so formed is such that $\Pi(S) \leqslant x^t$. Thus for $X = x^t$ we have $C(X) \geqslant X^{3B/5-\varepsilon}$ for all sufficiently large y. But $X = \exp(y^{1+\delta}\exp(y^{1+\delta/2}))$, so that $C(X) \geqslant X^{3B/5-\varepsilon}$ for all sufficiently large values of X. Since y can be uniquely determined from X, we complete the proof by taking $c_0 = EB/2$. □

References

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

[2] W. Banks, 'Carmichael numbers with a square totient', *Canad. Math. Bull.* **52** (1) (2009), no. 1, 3–8.

[3] W. Banks and C. Pomerance, 'On Carmichael numbers in arithmetic progressions', to appear in *J. Austral. Math. Soc.*

[4] D. A. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory, and complex multiplication.* John Wiley & Sons, Inc., New York, 1989.

[5] D. S. Dummit and R. M. Foote, *Abstract Algebra.* Third edition. John Wiley & Sons, Inc., Hoboken, NJ, 2004. xii+932 pp. ISBN: 0-471-43334-9

[6] A. Ekstrom, C. Pomerance, and D. S. Thakur, 'Infinitude of elliptic Carmichael numbers', preprint, 2011.

[7] J. B. Friedlander, 'Shifted primes without large prime factors', in *Number theory and applications* (ed. R. A. Mollin), (Kluwer, NATO ASI, 1989), 393–401.

[8] J. Grantham, 'There are infinitely many Perrin pseudoprimes', *J. Number Theory* **130** (2010), no. 5, 1117–1128.

[9] G. J. Janusz, *Algebraic number fields*, Pure and Applied Mathematics, Vol. 55., Academic Press [A Subsidiary of Harcourt Brace Jovanovich, Publishers], New York-London, 1973. x+220 pp.

[10] J. C. Lagarias and A. M. Odlyzko, 'Effective versions of the Chebotarev density theorem', in *Algebraic number fields: L-functions and Galois properties* (Proc. Sympos., Univ. Durham, Durham, 1975), 409–464.

[11] H. L. Montgomery and R. C. Vaughan, 'The large sieve', *Mathematika* **20** (1973), 119–134.

[12] K. Matomäki, 'Carmichael numbers in arithmetic progressions', preprint, 2011.

[13] J. Neukirch, *Algebraic number theory.* Grundlehren der Mathematischen Wissenschaften, **322**. Springer-Verlag, Berlin, 1999.

[14] J. B. Rosser and L. Schoenfeld, 'Approximate formulas for some functions of prime numbers', *Illinois J. Math.* **6** (1962), 64–94.

[15] L. C. Washington, *Introduction to cyclotomic fields.* Second edition. Graduate Texts in Mathematics, **83**. Springer-Verlag, New York, 1997.

[16] A. Weiss, 'The least prime ideal', *J. Reine Angew. Math.* **338** (1983), 56–94.

Department of Mathematics, University of Missouri, Columbia, MO 65211 USA
E-mail address: `bankswd@missouri.edu`

Department of Mathematics, Bilkent University, 06800 Bilkent, Ankara, TURKEY
E-mail address: `guloglua@fen.bilkent.edu.tr`

Department of Mathematics, University of Missouri, Columbia, MO 65211, USA
E-mail address: `amydm6@mail.missouri.edu`