Available online at www.sciencedirect.com
ScienceDirect
Journal of Number Theory 128 (2008) 910–917
JOURNAL OF Number Theory
www.elsevier.com/locate/jnt

Carmichael numbers in number rings

G. Ander Steele

Department of Mathematics and Statistics, Boston University, 111 Cummington street, Boston, MA 02215, USA

Received 2 October 2006; revised 11 March 2007

Communicated by C. Pomerance

Abstract

We generalize Carmichael numbers to ideals in number rings and prove a generalization of Korselt's Criterion for these Carmichael ideals. We investigate when Carmichael numbers in the integers generate Carmichael ideals in the algebraic integers of abelian number fields. In particular, we show that given any composite integer n, there exist infinitely many quadratic number fields in which n is not Carmichael. Finally, we show that there are infinitely many abelian number fields K with discriminant relatively prime to n such that n is not Carmichael in K.

1. Introduction

Fermat's Little Theorem, one of the most important results in elementary number theory, states that if p is prime, then

$$a^p \equiv a \pmod{p}$$

for all integers a. This result gives us the rudimentary Fermat Compositeness Test: If $a^n \not\equiv a \pmod{n}$ for some integer a, then n is composite. While this has the advantage of being computationally simple, it has the distinct disadvantage of failing for some composite n and choice of a. Take, for example, $n = 341 = 31 \cdot 11$ and $a = 2$. A quick computation tells us that $2^{341} \equiv 2 \pmod{341}$. Fortunately, we can also choose $a = 3$ to get $3^{341} \equiv 168 \pmod{341}$, thus proving that 341 is composite. We cannot always be so lucky. There are some composite n which fail this test no matter how we pick a. A *Carmichael number* is a composite integer n such that

E-mail address: ander@bu.edu.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2007.08.009

$a^n \equiv a \pmod{n}$ for all integers a. The smallest such number is 561. The existence of Carmichael numbers means that the converse of Fermat's Little Theorem fails. Even worse, the fact that there are infinitely many Carmichael numbers [1] means that the converse fails rather spectacularly. On the bright side, one can completely characterize all Carmichael numbers using Korselt's Criterion.

Theorem 1.1 *(Korselt's Criterion). A composite integer $n > 1$ is Carmichael if and only if n is squarefree and $p - 1 \mid n - 1$ for all primes $p \mid n$.*

Fermat's Little Theorem can be generalized to prime ideals in the ring of integers of an algebraic field. A natural question to ask is whether or not an analog of Carmichael numbers exists in such rings. We answer in the affirmative and generalize Korselt's Criterion to completely characterize what we call Carmichael ideals. In particular, we investigate when Carmichael numbers in $\mathbb{Z}$ generate Carmichael ideals in abelian extension fields of $\mathbb{Q}$.

Finally, we generalize Fermat's Little Theorem to Galois number fields in such a way that the converse holds true. More specifically, we prove that an odd composite number n cannot generate a Carmichael ideal in all Galois number fields. In particular, we show that n is not Carmichael in all quadratic extensions of $\mathbb{Q}$. This argument depends on picking a number field K whose discriminant shares a common factor with n, but in certain cases we can show that n is not Carmichael in infinitely many quadratic number fields with discriminant relatively prime to n. In general this is not true, and we give an explicit example due to Howe of an integer n which is Carmichael in all quadratic number fields having discriminant relatively prime to n. However, we show that for every n there are infinitely many abelian number fields K with discriminant relatively prime to n such that n is not Carmichael in K. Finally, we show that if n is the product of at least three distinct primes, then there are infinitely many cyclotomic fields of prime conductor in which n is not Carmichael and n is relatively prime to the discriminant.

2. Extension fields

Let K be a number field (i.e., a finite extension field of $\mathbb{Q}$), and let $\mathcal{O}_K$ denote the ring of algebraic integers in K. If $\mathfrak{p}$ is a nonzero prime ideal in $\mathcal{O}_K$, then for all $\alpha \in \mathcal{O}_K$ we have

$$\alpha^{\mathrm{N}(\mathfrak{p})} \equiv \alpha \pmod{\mathfrak{p}} \tag{1}$$

where $\mathrm{N}(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$. This follows from the fact that nonzero prime ideals in $\mathcal{O}_K$ are maximal and thus the quotient $\mathcal{O}_K/\mathfrak{p}$ is a field. Therefore, the set of nonzero elements of $\mathcal{O}_K/\mathfrak{p}$ forms a group under multiplication. Equality (1) now follows from Lagrange's theorem.

As is the case in $\mathbb{Z}$, the converse of (1) is not true: there exist composite ideals for which (1) is satisfied for all $\alpha \in \mathcal{O}_K$. For example, 561 is not only Carmichael in $\mathbb{Z}$, it is also Carmichael in the ring $\mathcal{O}_K = \mathbb{Z}[\sqrt{-13}]$ of algebraic integers of $K = \mathbb{Q}(\sqrt{-13})$. In other words, the ideal (561) in $\mathcal{O}_K$ has the property that if $\alpha \in \mathcal{O}_K$, then

$$\alpha^{\mathrm{N}(561)} \equiv \alpha \pmod{(561)}.$$

We define Carmichael ideals as follows:

Definition 2.1. Let K be an extension field of $\mathbb{Q}$ and let $\mathfrak{n}$ be a composite ideal in $\mathcal{O}_K$. We say that $\mathfrak{n}$ is Carmichael in $\mathcal{O}_K$ if for all α in $\mathcal{O}_K$ we have

$$\alpha^{\mathrm{N}(\mathfrak{n})} \equiv \alpha \pmod{\mathfrak{n}}.$$

Remark. If a Carmichael ideal $\mathfrak{n}$ has norm $\mathrm{N}(\mathfrak{n}) > 2$, then $\mathrm{N}(\mathfrak{n})$ is odd: simply take $\alpha = -1$.

A natural question to ask is whether or not we can characterize Carmichael ideals with something along the lines of Korselt's Criterion. The following result answers this question affirmatively:

Theorem 2.2 *(Generalized Korselt Criterion). A composite ideal* $\mathfrak{n}$ *is Carmichael in* $\mathcal{O}_K$ *if and only if*

(1) $\mathfrak{n}$ *is squarefree, and*
(2) $\mathrm{N}(\mathfrak{p}) - 1 \mid \mathrm{N}(\mathfrak{n}) - 1$ *for all prime ideals* $\mathfrak{p} \mid \mathfrak{n}$.

Proof. We begin with the easier direction: Suppose for all $\mathfrak{p} \mid \mathfrak{n}$, we have $\mathrm{N}(\mathfrak{p}) - 1 \mid \mathrm{N}(\mathfrak{n}) - 1$. We know that for $\alpha \in \mathcal{O}_K$ and $\alpha \notin \mathfrak{p}$, $\alpha^{\mathrm{N}(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}}$. If $\mathfrak{p} \mid \mathfrak{n}$, we thus have $\forall \alpha \notin \mathfrak{p}$, $\alpha^{(\mathrm{N}(\mathfrak{n})-1)} \equiv 1 \pmod{\mathfrak{p}}$. Therefore, $\forall \alpha \in \mathcal{O}_K$, $\alpha^{\mathrm{N}(\mathfrak{n})} \equiv \alpha \pmod{\mathfrak{p}}$. Using the fact that $\mathfrak{n}$ is squarefree and applying the Chinese Remainder Theorem, we have $\alpha^{\mathrm{N}(\mathfrak{n})} \equiv \alpha \pmod{\mathfrak{n}}$, hence $\mathfrak{n}$ is Carmichael in $\mathcal{O}_K$.

Now assume that $\mathfrak{n}$ is Carmichael in $\mathcal{O}_K$. Suppose that $\mathfrak{n} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r}$. Since $\mathfrak{n}$ is Carmichael, we have $\alpha^{\mathrm{N}(\mathfrak{n})} \equiv \alpha \pmod{\mathfrak{p}_i}$ for all $\alpha \in \mathcal{O}_K$. Choosing α not in $\mathfrak{p}_i$, we see $\alpha^{\mathrm{N}(\mathfrak{n})-1} \equiv 1 \pmod{\mathfrak{p}_i}$. Therefore, the order of α mod $\mathfrak{p}_i$ divides $\mathrm{N}(\mathfrak{n}) - 1$. Also $(\mathcal{O}_K/\mathfrak{p}_i)^*$ is the multiplicative group of a finite field, and therefore has an element of order $\mathrm{N}(\mathfrak{p}_i) - 1$. It follows that $\mathrm{N}(\mathfrak{p}_i) - 1 \mid \mathrm{N}(\mathfrak{n}) - 1$.

Finally, we show that $\mathfrak{n}$ is squarefree if it is Carmichael. Suppose we have a prime ideal $\mathfrak{p}$ such that $\mathfrak{p}^2 \mid \mathfrak{n}$. The group of units of the quotient $\mathcal{O}_K/\mathfrak{p}^2$ has cardinality $\mathrm{N}(\mathfrak{p})(\mathrm{N}(\mathfrak{p}) - 1)$. If p is the prime lying below $\mathfrak{p}$, then $p \mid \mathrm{N}(\mathfrak{p})$, so p divides the order of the group $(\mathcal{O}_K/\mathfrak{p}^2)^*$. By Cauchy's theorem, there exists an element α of $(\mathcal{O}_K/\mathfrak{p}^2)^*$ with order p. This yields a contradiction, since the fact that $\mathfrak{n}$ is Carmichael implies that $\alpha^{\mathrm{N}(\mathfrak{n})-1} \equiv 1 \pmod{\mathfrak{p}^2}$, but $p \nmid \mathrm{N}(\mathfrak{n}) - 1$. Therefore, $\mathfrak{n}$ is squarefree. □

Remark. The usual version of Korselt's Criterion follows from Theorem 2.2 by considering $K = \mathbb{Q}$.

An immediate consequence of the Generalized Korselt Criterion is the following generalization of Fermat's Little Theorem:

Theorem 2.3. *Let* p *be prime. Then if* K *is a Galois extension of* $\mathbb{Q}$ *such that* $p \nmid \mathrm{Disc}(K)$,

$$\alpha^{\mathrm{N}(p)} \equiv \alpha \pmod{p}$$

for all $\alpha \in \mathcal{O}_K$. *In particular, the ideal* $p\mathcal{O}_K$ *is either prime or Carmichael.*

Proof. Since $p \nmid \mathrm{Disc}(K)$, and $K/\mathbb{Q}$ is Galois, we have $(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, the product of distinct prime ideals each with norm $\mathrm{N}(\mathfrak{p}_i) = p^f$. We have $r \cdot f = [K : \mathbb{Q}]$, and thus $\mathrm{N}(\mathfrak{p}_i) - 1 = p^f - 1 \mid p^{[K:\mathbb{Q}]} - 1 = \mathrm{N}(p) - 1$ for all $\mathfrak{p}_i \mid (p)$. Therefore, the ideal (p) satisfies the Generalized Korselt Criterion and the theorem is proved. □

The nice thing about this generalization of Fermat's Little Theorem is that the converse is actually true! That is to say, if n is Carmichael in all Galois extensions K such that $n \nmid \mathrm{Disc}(K)$, then n must be prime. In fact, we prove that quadratic extensions suffice.

Theorem 2.4 *(Converse of Theorem 2.3). Let $n > 2$ be composite. Then there exists a quadratic extension K of $\mathbb{Q}$ with $n \nmid \mathrm{Disc}(K)$ and an element $\alpha \in \mathcal{O}_K$ such that*

$$\alpha^{\mathrm{N}(n)} \not\equiv \alpha \pmod{n}.$$

Proof. If n is not squarefree, then the ideal (n) is never squarefree in any abelian extension K and thus cannot be Carmichael by the Generalized Korselt Criterion.

On the other hand, suppose n is the product of distinct primes. Then n must have an odd prime divisor. Fix an odd prime p dividing n, and let $K = \mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$. As p ramifies in K, we have $(p) = \mathfrak{p}^2$ and thus the ideal (n) in $\mathcal{O}_K$ is not squarefree. Therefore, n is not Carmichael in K. Furthermore, $\mathrm{Disc}(K) = p$ so $n \nmid \mathrm{Disc}(K)$. □

More generally, the above argument shows that a number n will fail to be Carmichael in any number field K such that $(n, \mathrm{Disc}(K)) \neq 1$. In particular, a composite number n will not generate a squarefree ideal in $\mathcal{O}_K$ if a prime factor of n ramifies in K. Note that the condition $p \nmid \mathrm{Disc}(K)$ in Theorem 2.3 has two possible generalizations for composite n. We can require, as in the case of Theorem 2.4, that $n \nmid \mathrm{Disc}(K)$, or we can impose the stronger requirement that n is relatively prime to $\mathrm{Disc}(K)$. In certain cases, we can show that n is not Carmichael in infinitely many quadratic extensions with discriminant *relatively prime* to n.

Theorem 2.5. *Suppose that n is odd, squarefree, and that*

$$p^2 - 1 \nmid n^2 - 1 \text{ for some odd prime } p \mid n. \tag{2}$$

Then there exist infinitely many quadratic fields $K = \mathbb{Q}(\sqrt{d})$ such that $(n, \mathrm{Disc}(K)) = 1$ and n is not Carmichael in K.

Proof. Consider the set S of integers d satisfying

(1) d is relatively prime to n/p,
(2) d is a quadratic non-residue modulo p,
(3) $d \equiv 1 \pmod 4$.

These conditions are simply congruence relations modulo n/p, p, and 4, respectively. By hypothesis, n/p, p, and 4 are relatively prime, thus the Chinese Remainder Theorem implies S has positive density. Now consider the set $S' \subseteq S$ of elements which are squarefree. We claim that this set is nonempty. Indeed, any element d of S can be written as $d = e \cdot f^2$, where $e, f \in \mathbb{Z}$ and e is squarefree. Observe that e satisfies conditions (1)–(3) and so e is an element of S'. If S'

were finite, then S would be contained in the set $\{s \cdot f^2 \mid s \in S',\ f \in \mathbb{Z}\}$, which has density 0. Therefore, S' is infinite.

Fix d in S', and let $K = \mathbb{Q}(\sqrt{d})$. The prime p remains inert in K, and thus $\mathfrak{p} = (p)$ is prime, divides (n), and has norm $\mathrm{N}(\mathfrak{p}) = p^2$. Therefore, $\mathrm{N}(\mathfrak{p}) - 1 = p^2 - 1$ does not divide $n^2 - 1 = \mathrm{N}(n) - 1$ and by the Generalized Korselt Criterion, n is not Carmichael in K. Moreover, $\mathrm{Disc}(K) = d$ is relatively prime to n. □

Thus we see that if n satisfies (2), then n fails to be Carmichael in a much larger set of quadratic number fields than just the ones for which $(n, \mathrm{Disc}(K)) > 1$. This theorem is illustrated by the following example:

Example 2.6. Consider the ideal generated by 561 in the ring of integers $\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$ of $\mathbb{Q}(\sqrt{13})$. If we let $\alpha = 2 + \frac{1+\sqrt{13}}{2} \in \mathbb{Z}[\frac{1+\sqrt{13}}{2}]$, then

$$\alpha^{\mathrm{N}(561)} \equiv 512 + 154\frac{1+\sqrt{13}}{2} \not\equiv \alpha \pmod{(561)}.$$

Since 561 does not satisfy Fermat's Little Theorem in $\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$ and does not divide $\mathrm{Disc}(K) = 13$, we have proven that 561 is composite. Furthermore, 561 is relatively prime to 13, so we have proven the compositeness of 561 without explicitly using a prime factor of 561 in the computation.

Unfortunately, it is possible for a composite integer n to be Carmichael in all quadratic extensions K having discriminant relatively prime to n. If n is composite and $p^2 - 1 \mid n^2 - 1$ for all primes $p \mid n$, then n is Carmichael in all quadratic number rings with discriminant relatively prime to n. In fact, a more general statement is true:

Theorem 2.7. *Suppose n is squarefree and that $p^i - 1 \mid n^d - 1$ for all primes $p \mid n$ and all $0 < i \leqslant d$. Then if $K/\mathbb{Q}$ is a degree-d extension with discriminant relatively prime to n, n is Carmichael in K.*

Proof. If n is relatively prime to $\mathrm{Disc}(K)$, then none of the prime factors of n ramify in K. Therefore, the ideal (n) is squarefree. Let $\mathfrak{p}$ be a prime ideal dividing (n). If $(p) = \mathfrak{p} \cap \mathbb{Z}$ is the prime lying below $\mathfrak{p}$, then we have that $p \mid n$ and $\mathrm{N}(\mathfrak{p}) = p^s$ for some $0 < s \leqslant d$. By hypothesis, $\mathrm{N}(\mathfrak{p}) - 1 = p^s - 1$ divides $\mathrm{N}(n) - 1 = n^d - 1$. The Generalized Korselt Criterion implies n is Carmichael in K. □

In the case of quadratic extensions, it is possible to give examples of composite n which satisfy the conditions of Theorem 2.7. Howe gives $n = 17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331$, which is also an example of what he calls a *rigid Carmichael numbers of order 2* [4]. In fact, Howe's rigid Carmichael numbers of order d are exactly the composite n that satisfy the conditions of Theorem 2.7.

We will show that even if n is a rigid Carmichael number of order 2, it fails to be Carmichael in some higher degree abelian extensions with discriminant coprime to n. On the other hand, heuristics in [4] suggest that there are infinitely many rigid Carmichael numbers of order d for any $d \geqslant 2$. If n is a rigid Carmichael number of order d then Theorem 2.7 implies that n is

Carmichael in all number fields of degree $\leqslant d$ with discriminant coprime to n. However, Theorem 3.1 (below) shows that for any composite n, we have infinitely many number fields in which n is not Carmichael and the discriminant is relatively prime to n.

3. Cyclotomic fields

The abelian extensions of $\mathbb{Q}$ are precisely the subfields of cyclotomic fields. We have shown that a generalization of Fermat's Little Theorem is true for Galois number fields, as long as the prime p does not divide the discriminant of the number field. We have also shown that the converse of this generalized Fermat's Little Theorem is true, and that a composite number n will fail the first part of the Generalized Korselt Criterion in infinitely many quadratic extensions. Now, using subfields of cyclotomic fields, we show any composite number n will fail the second part of the Generalized Korselt Criterion in infinitely many abelian number fields. In particular, we have the following theorem:

Theorem 3.1. *Let n be composite. Then there exist infinitely many abelian number fields K such that n is relatively prime to* $\mathrm{Disc}(K)$ *and n is not Carmichael in K.*

In order to prove this theorem, we require a few lemmas.

Lemma 3.2. *Let p be prime and $G = (\mathbb{Z}/p\mathbb{Z})^*$. Suppose n is not divisible by p and $d = \mathrm{ord}_p(n)$ is relatively prime to $\frac{p-1}{d}$. If $H \leqslant G$ is the subgroup of order $\frac{p-1}{d}$, then the image of n generates the quotient group G/H.*

Proof. Let g be a generator of G. Then $H = \langle g^d \rangle$. Since n has order d, $n = g^{a(p-1)/d}$, where a is relatively prime to d. The order of n in G/H is the smallest integer k such that $n^k \in H$. If k is the order of n in G/H, then $n^k = g^{ak(p-1)/d} \in H$ and $g^{ak(p-1)/d} = (g^d)^s = g^{ds}$ for some integer s. Thus $ak(p-1)/d \equiv ds \pmod{p-1}$. Since $d \mid p-1$, we have $d \mid ak(p-1)/d$. Since d is relatively prime to a and $(p-1)/d$, $d \mid k$. Therefore, the order of n in G/H is d and thus the image of n generates G/H. □

Lemma 3.3. *If $n \in \mathbb{N}$ is divisible by at least two distinct primes, p and q, then there exists d_0 such that $p^d - 1 \nmid n^d - 1$ for all $d > d_0$.*

Proof. Bugeaud, Corvaja, and Zannier show that $(p^d - 1, n^d - 1) \ll p^{d/2} < p^d - 1$, for large d [2]. Thus, there exists some d_0 such that $p^d - 1 \nmid n^d - 1$ for all $d > d_0$. □

Lemma 3.4. *There are infinitely many primes p such that $p - 1$ is squarefree.*

Proof. This is a "well-known" fact which follows, for example, from Theorem 2 in Mirsky's paper [5]. □

Proof of Theorem 3.1. If n is a prime power, then (n) is never squarefree and we are done. Now suppose n is not a prime power. Let p be a prime divisor of n. By Lemma 3.3, there exists an integer d_0 such that $p^d - 1 \nmid n^d - 1$ for all $d > d_0$. Thus, if K is a number field of degree d greater than d_0 and p remains inert in K, we have

$$\mathrm{N}(p) - 1 = p^d - 1 \nmid n^d - 1 = \mathrm{N}(n) - 1$$

and thus n is not Carmichael by the Generalized Korselt Criterion. By taking $q > p^{d_0} - 1$, it follows from Lemma 3.4 that there are infinitely many primes q such that $q - 1$ is squarefree and the order of p modulo q is greater than d_0. If we fix such a q and let $E = \mathbb{Q}(\zeta_q)$, the Galois group of $E/\mathbb{Q}$ is isomorphic to $G = (\mathbb{Z}/q\mathbb{Z})^*$. Let d denote the order of p modulo q and let $H < G$ be the subgroup of order $\frac{p-1}{d}$. If we let $K = \mathrm{Fix}(H)$ be the fixed field of H, then the Galois group of $K/\mathbb{Q}$ is G/H. Lemma 3.2 shows that p generates the quotient group G/H and thus p remains inert in K, which has degree $d > d_0$. It follows that n is not Carmichael in K for infinitely many K with discriminant relatively prime to n. □

By using a difficult analytic result due to Heath-Brown, one can prove an analog of Theorem 3.1 using only cyclotomic fields.

Theorem 3.5 *(Heath-Brown). All primes, with the possible exception of at most two, are primitive roots for infinitely many primes p.*

Proof. See [3]. □

One can apply Lemma 3.3, along with Theorem 3.5, to obtain the following theorem:

Theorem 3.6. *Let n be the product of at least three distinct primes. Then there exist infinitely many cyclotomic extensions of the form $K = \mathbb{Q}(\zeta_q)$, where q is prime, such that n is relatively prime to* $\mathrm{Disc}(K)$ *and n is not Carmichael in K.*

Proof. By hypothesis, n has at least three prime factors, so by Theorem 3.5 some prime $p \mid n$ is a primitive root for infinitely many primes q. Lemma 3.3 implies there exists some $d_0 \in \mathbb{N}$ such that $p^d - 1 \nmid n^d - 1$ for all $d > d_0$. There exist infinitely many $q > d_0$ relatively prime to n such that p is a primitive root modulo q. If we fix any such q and let $K = \mathbb{Q}(\zeta_q)$, then $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/q\mathbb{Z})^*$. The prime p remains inert in K since it generates $(\mathbb{Z}/q\mathbb{Z})^*$, and thus we have

$$\mathrm{N}(p) - 1 = p^{q-1} - 1 \nmid n^{q-1} - 1 = \mathrm{N}(n) - 1.$$

By the Generalized Korselt Criterion, n is not Carmichael in K. Therefore, n is not Carmichael in infinitely many cyclotomic extensions with discriminant relatively prime to n. □

It is a well-known fact that Carmichael numbers in $\mathbb{Z}$ are divisible by at least three distinct primes. Therefore, we see all composite n fail to be Carmichael in at least one cyclotomic field.

Corollary 3.7. *Let n be a composite integer. Then there exists at least one cyclotomic extension of the form $K = \mathbb{Q}(\zeta_q)$, where q is prime, such that n is relatively prime to* $\mathrm{Disc}(K)$ *and n is not Carmichael in K.*

Proof. If n is a prime power, then n is not squarefree and thus is never Carmichael in any number field. If n is the product of two distinct primes, then n is not Carmichael in $K = \mathbb{Q}(\zeta_2) = \mathbb{Q}$, which has $\mathrm{Disc}(K) = 1$. If n is the product of at least three distinct primes, then Theorem 3.6 gives us the result. □

Acknowledgments

This research was supported by the Georgia Institute of Technology School of Mathematics NSF VIGRE-funded REU program, and by Dr. Matthew Baker's NSF grant DMS-0600027. Thanks to Dr. Keith Conrad for posing the question that started this project and for his advice. Thanks to Ernest Croot for suggesting [3] and for his advice. Special thanks to Dr. Baker for his invaluable guidance and support. Finally, thanks to the anonymous referee for many useful suggestions, including simplifications to the proofs of Theorems 2.4 and 2.5.

References

[1] W.R. Alford, Andrew Granville, Carl Pomerance, There are infinitely many Carmichael numbers, Ann. of Math. (2) 139 (3) (1994) 703–722.
[2] Y. Bugeaud, P. Corvaja, U. Zannier, An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$, Math. Z. 243 (1) (2003) 79–84.
[3] D.R. Heath-Brown, Artin's conjecture for primitive roots, Quart. J. Math. Oxford Ser. (2) 37 (145) (1986) 27–38.
[4] Everett W. Howe, Higher-order Carmichael numbers, Math. Comp. 69 (232) (2000) 1711–1719.
[5] L. Mirsky, The number of representations of an integer as the sum of a prime and a k-free integer, Amer. Math. Monthly 56 (1949) 17–19.