Journal of Number Theory 165 (2016) 15–29

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Carmichael numbers and the sieve

William D. Banks [a,*], Tristan Freiberg [b]

[a] *Department of Mathematics, University of Missouri, Columbia MO, USA*
[b] *Department of Pure Mathematics, University of Waterloo, Waterloo ON, Canada*

A R T I C L E I N F O

Article history:
Received 3 July 2015
Received in revised form 30 November 2015
Accepted 9 January 2016
Available online 4 March 2016
Communicated by R.C. Vaughan

Dedicated to Carl Pomerance on the occasion of his 70th birthday

Keywords:
Carmichael numbers
Semi-linear sieve

A B S T R A C T

As an application of the semi-linear sieve, we show that there are infinitely many Carmichael numbers whose prime factors all have the form $p = 1 + a^2 + b^2$, where the integers a and b are coprime.

© 2016 Elsevier Inc. All rights reserved.

1. Introduction

For any prime number n, Fermat's little theorem asserts that

$$a^n \equiv a \ (n) \qquad (a \in \mathbb{Z}). \tag{1.1}$$

Around 1910, Carmichael initiated the study of composite numbers n with the property (1.1); these are now known as *Carmichael numbers*. The existence of infinitely many Carmichael numbers was first established in the celebrated 1994 paper of Alford, Granville and Pomerance [1].

* Corresponding author.
E-mail addresses: bankswd@missouri.edu (W.D. Banks), tfreiberg@uwaterloo.ca (T. Freiberg).

http://dx.doi.org/10.1016/j.jnt.2016.01.012
0022-314X/© 2016 Elsevier Inc. All rights reserved.

Since prime numbers and Carmichael numbers are linked by the common property (1.1), from a number-theoretic point of view it is natural to investigate various arithmetic properties of Carmichael numbers. For example, Banks and Pomerance [9] gave a conditional proof of their conjecture that there are infinitely many Carmichael numbers in an arithmetic progression $a + bc$ ($c \in \mathbb{Z}$) whenever $(a, b) = 1$. The conjecture was proved unconditionally by Matomäki [21] in the special case that a is a quadratic residue modulo b, and using an extension of her methods Wright [25] established the conjecture in full generality. The techniques introduced in [1] have led to many other investigations into the arithmetic properties of Carmichael numbers; see [2–5,7,8,10,15–20,22,24] and the references therein.

In this paper, we combine sieve techniques with the method of [1] to prove the following result.

Theorem 1.1. *There exist infinitely many Carmichael numbers whose prime factors all have the form $p = 1 + a^2 + b^2$ with some $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$. Moreover, there is a positive constant C such that the number of such Carmichael numbers not exceeding x is at least x^C (once x is sufficiently large).*

Remark 1.2. The Carmichael numbers described in this theorem are somewhat unusual. Up to 10^9, there are only three such Carmichael numbers, namely 561, 162 401 and 221 884 001. By contrast, there are 646 "ordinary" Carmichael numbers up to 10^9.

As is well known, whenever $p = 6k+1$, $q = 12k+1$ and $r = 18k+1$ are simultaneously prime for some positive integer k, the number $n = pqr$ is a Carmichael number. However, no number of this form is a Carmichael number of the type described in the theorem, since $p-1 = 6k$ and $r-1 = 3 \cdot 6k$ cannot both be expressed as a sum of two squares. □

Let $\mathbb{P}_*$ be the set of primes of the form $p = 1 + a^2 + b^2$, where a and b are coprime integers. The idea underlying our proof of Theorem 1.1 is to show that $\mathbb{P}_*$ is sufficiently well-distributed over certain arithmetic progressions so that, following the method of Alford, Granville and Pomerance [1], the primes used to construct Carmichael numbers can all be drawn from $\mathbb{P}_*$. The semi-linear sieve (see, e.g., Friedlander and Iwaniec [14]) provides good estimates for the number of primes $p \in \mathbb{P}_*$ not exceeding x; however, following [1] we further require decent upper and lower bounds for the number of such primes in certain arithmetic progressions of the form 1 modulo d, where d can be as large as a fixed positive power of x. Fortunately, this is needed only for certain moduli d that are fairly smooth and not divisible by an exceptional modulus. Consequently, to achieve the desired bounds we apply the semi-linear sieve to the set of primes $p \leqslant x$ with $p \equiv 1$ (d) using a modified version of the Bombieri–Vinogradov theorem derived from Banks et al. [6, Theorem 4.1]; see Theorem 3.3 below.

Theorem 1.1 asserts the existence of infinitely many Carmichael numbers whose prime factors all have the form $p = 1 + \Phi(a, b)$, where $a, b \in \mathbb{Z}$ and $\Phi(x, y) = x^2 + y^2$. In principle, our methods can be adapted to obtain similar results with other positive

Download English Version:

https://daneshyari.com/en/article/4593238

Download Persian Version:

https://daneshyari.com/article/4593238

Daneshyari.com