COUNTING CARMIŁEAN NUMBERS WITH SMALL SEEDS

ZHENXIANG ZHANG

Abstract. Let $A_s$ be the product of the first $s$ primes, let $\mathcal{P}_s$ be the set of primes $p$ for which $p-1$ divides $A_s$ but $p$ does not divide $A_s$, and let $\mathcal{C}_s$ be the set of Carmichael numbers $n$ such that $n$ is composed entirely of the primes in $\mathcal{P}_s$ and such that $A_s$ divides $n-1$. Erdős argued that, for any $\varepsilon > 0$ and all sufficiently large $x$ (depending on the choice of $\varepsilon$), the set $\mathcal{C}_s$ contains more than $x^{1-\varepsilon}$ Carmichael numbers $\leq x$, where $s$ is the largest number such that the $s$th prime is less than $\ln x^{\varepsilon}/4$. Based on Erdős’s original heuristic, though with certain modification, Alford, Granville, and Pomerance proved that there are more than $x^{2/7}$ Carmichael numbers up to $x$, once $x$ is sufficiently large.

The main purpose of this paper is to give numerical evidence to support the following conjecture which shows that $|\mathcal{C}_s|$ grows rapidly on $s$: $|\mathcal{C}_s| = 2^{2^{s(1-\varepsilon)}}$ with $\lim_{s \to \infty} \varepsilon = 0$, or, equivalently, $|\mathcal{C}_s| = A_2^{2^{s(1-\varepsilon')}}$ with $\lim_{s \to \infty} \varepsilon' = 0$. We describe a procedure to compute exact values of $|\mathcal{C}_s|$ for small $s$. In particular, we find that $|\mathcal{C}_9| = 8,281,366,855,879,527$ with $\varepsilon = 0.36393\ldots$ and that $|\mathcal{C}_{10}| = 21,823,464,288,660,480,291,170,614,377,509,316$ with $\varepsilon = 0.31662\ldots$. The entire calculation for computing $|\mathcal{C}_s|$ for $s \leq 10$ took about 1,500 hours on a PC Pentium Dual E2180/2.0GHz with 1.99 GB memory and 36 GB disk space.

1. Introduction

Let $b_i$ be the $i$th prime. Let $s \geq 1$ and let $A_s = \prod_{i=1}^{s} b_i$ be the product of the first $s$ primes. It is easy to see that (as Erdős [4] knew)

$$A_s < e^{2b_s}.$$ (1.1)

Define sets

$$\mathcal{P}_s = \{\text{prime } p : p > b_s, \: p-1|A_s\},$$ (1.2)

$$\mathcal{N}_s = \{n > 1 : n \text{ is square free and composed entirely of the primes in } \mathcal{P}_s\},$$ (1.3)

and

$$\mathcal{C}_s = \{n \in \mathcal{N}_s : A_s|n-1, \: n-1 \neq A_s\}.$$ (1.4)

By Korselt’s criterion [6] (see also [3] Section 3.4.2)), every number $n \in \mathcal{C}_s$ is Carmichael [2]. Since the sets $\mathcal{P}_s, \mathcal{N}_s$, and $\mathcal{C}_s$ are determined by the first $s$ primes, we say that these sets are generated by the (square-free) (prime) seeds $b_1, \ldots, b_s$.

Received by the editor October 19, 2009 and, in revised form, October 28, 2009.

2010 Mathematics Subject Classification. Primary 11Y16, 11Y35; Secondary 11Y11.

Key words and phrases. Carmichael numbers (with small seeds), Korselt’s criterion, heuristics of Erdős-AGP concerning Erdős’s construction of Carmichael numbers, product of the first $s$ primes, algorithms.

The author was supported by the NSF of China Grant 10071001.
Erdős [4] argued that, for any $\varepsilon > 0$ and all sufficiently large $x$ (depending on the choice of $\varepsilon$), the set $C_s$ contains more than $x^{1-\varepsilon}$ Carmichael numbers $\leq x$, where $s$ is the largest number such that $b_s < \ln x^{\varepsilon/4}$. In short, Erdős [4] made the following Conjecture.

**Conjecture 1** (Erdős).
There are $x^{1-o(1)}$ Carmichael numbers up to $x$.

Based on Erdős’s original heuristic [4], though with certain modification, Alford, Granville, and Pomerance [1] proved the following Theorems.

**Theorem 1** (Alford, Granville, and Pomerance).
There are more than $x^{2/7}$ Carmichael numbers up to $x$, once $x$ is sufficiently large.

**Theorem 2** (Alford, Granville, and Pomerance).
Fix $\varepsilon > 0$. Assume that, for sufficiently larger $x$, the arithmetic progression $1 \pmod{d}$ contains more than $x/(2d \ln x)$ primes up to $x$ provided $d < x^{1-\varepsilon}$. Then there are more than $x^{1-2\varepsilon}$ Carmichael numbers up to $x$, once $x$ is sufficiently large.

Note that the counts of the number of Carmichael numbers in either Conjecture or Theorems are functions which grow slowly on $x$. For $x = 10^n$ for $n$ up to 21 (which is as far as has been computed [7]), there are fewer than $x^{0.348}$ Carmichael numbers up to $x$.

The main purpose of this paper is to give numerical evidence to support the following Conjecture which shows that $|C_s|$ grows rapidly on $s$.

**Conjecture 2.** We have

\begin{equation}
|C_s| = 2^{2^{s(1-\varepsilon)}}
\end{equation}

with $\lim_{s \to \infty} \varepsilon = 0$, or, equivalently,

\begin{equation}
|C_s| = A_s^{2^{s(1-\varepsilon')}}
\end{equation}

with $\lim_{s \to \infty} \varepsilon' = 0$.

In Section 2, we first briefly state reasons for making Conjecture which are essentially based on the heuristics of Erdős, Alford, Granville, and Pomerance concerning Erdős’s construction of Carmichael numbers. Then we describe a procedure for finding $|C_s|$ for small $s$ and tabulate $|C_s|$ and relative values for $3 \leq s \leq 10$. In particular, we have $|C_9| = 8, 281, 366, 855, 879, 527$ with $\varepsilon = 0.36393\ldots$ and

$|C_{10}| = 21, 823, 464, 288, 660, 480, 291, 170, 614, 377, 509, 316$

with $\varepsilon = 0.31662\ldots$. The entire calculation for $|C_s|$ for $s \leq 10$ took about 1,500 hours on a PC Pentium Dual E2180/2.0GHz with 1.99 GB memory and 36 GB disk space.

**Remark 1.1.** Alford (see [5]) took $L = 2^5 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11$, determined 155 primes $p$ for which $p - 1$ divides $L$, and then established that there are at least $2^{128} - 1$ Carmichael numbers made up from them. However, Alford did not express the number of Carmichael numbers as a function of $L$. Granville [5] mentioned: “It can be shown that if $L = A_s$ for some sufficiently large $s$, then we can obtain more than $2 \ln^2 L$ primes in $P_s$, and so we’d expect more than

\begin{equation}
L \ln^2 L
\end{equation}

Carmichael numbers in $C_s$.” The estimate seems to be the only estimate for $|C_s|$ in the literature, which grows much more slowly than that in Conjecture.
2. Evaluating $|C_s|$

Since the probability of a number $\leq m$ to be prime is greater than $1/\ln m$ and since $A_s$ has $2^{s-1}$ even divisors, it is reasonable to conjecture that

$$|P_s| = 2^s \left(1+o(1)\right).$$

Given $s \geq 3$, let $Z_{A_s} = \{0, 1, 2, \ldots, A_s - 1\}$ and let

$$Z_{A_s}^* = \{r \in Z_{A_s} : \gcd(A_s, r) = 1\} = \{1 < u_1 < u_2 < \ldots < u_{\varphi(A_s)}\},$$

where $\varphi(\cdot)$ is the Euler function. Define the set

$$R_s = \{r \in Z_{A_s} : r \equiv n \pmod{A_s} \text{ for some } n \in N_s\}.$$ Then $R_s \subseteq Z_{A_s}^*$ and $|R_s| \leq \varphi(A_s)$. For $r \in Z_{A_s}^*$, define the function

$$f_s(r) = \#\{n \in N_s : n \equiv r \pmod{A_s}\}.$$ Then we have

$$|C_s| = \begin{cases} f_s(1) - 1, & \text{if } A_s + 1 \in P_s; \\ f_s(1), & \text{otherwise.} \end{cases}$$

Let

$$a_s = \frac{|N_s|}{\varphi(A_s)} = \frac{2^{|P_s|} - 1}{\varphi(A_s)},$$

$$g_{s,1} = \min\{f_s(r) : r \in Z_{A_s}^*\}, \quad g_{s,2} = \min\{f_s(r) : r \in Z_{A_s}^*\}.$$ Let $\beta_s$ be such that

$$g_{s,1} - g_{s,2} = a_s^{\beta_s}.$$ Numerical evidence (see Table 1) suggests that

$$\beta_s < 0.6 \text{ for } s \geq 8,$$

which implies that

$$g_{s,1} - g_{s,2} = o(a_s) \quad \text{and} \quad \lim_{s \to \infty} g_{s,2}/g_{s,1} = \lim_{s \to \infty} |C_s|/a_s = 1.$$ Note that (2.6) gives an explicit and extended version of Erdős’s argument [4] that members of the set $N_s$ are roughly equi-distributed mod $A_s$.

Combining (2.3), (1.1), (2.1), and (2.6), we have Conjecture 2. Based on (2.3), we use the following procedure to compute $|C_s|$ for small $s$.

**PROCEDURE 1.** Finding $|C_s|$:
{\input{procedure1.tex}}

**BEGIN** Compute $A_s$ and $\varphi(A_s)$;

Determine the set $P_s = \{p_1 < p_2 < ... < p_m\}$;

For $r := 1$ To $A_s - 1$ Do

begin If $\gcd(A_s, r) = 1$ Then Begin $i \leftarrow i + 1; u_i \leftarrow r; h_r \leftarrow i$ End end;

For $i := 1$ To $\varphi(A_s)$ Do $H(i) \leftarrow 0$;

$i \leftarrow 1; t \leftarrow 1; H(h_{p_i}) \leftarrow 1$;

Repeat $i \leftarrow i + 1; p \leftarrow p_i \pmod{A_s}; H_0 \leftarrow H$;

For $j := 1$ To $\varphi(A_s)$ Do

begin If $H_0(j) > 0$ Then
Remark 2.1. For \(s \leq 9\), we save the set \(\{u_i\}\) (see (2.2)) in an array with each entry 4 bytes, which takes \(\varphi(A_s) \cdot 4 = 145,981,440\) bytes of memory, and save the set \(\{h_r : 1 \leq r < A_s, h_r = i\text{ if } r = u_i\}\) also in an array with each entry 4 bytes, which takes \((A_9 - 1) \cdot 4 = 892,371,476\) bytes of memory, since \(A_9 = 223,092,870\)
\[ \eta \text{ and } \phi \text{ and } \varphi \text{ of } A_9 \text{ could not be saved in the memory of my PC. They are saved in disk files. Since } A_9 = 6, 469, 693, 230 > 2^{32}, \text{ neither the set } \{h_r\} \text{ nor the set } \{u_i\} \text{ could be fit in the 1.99 GB of memory of my PC. We have to take a new approach for } s = 10 \text{ different from that for } s \leq 9. \text{ Note that } A_8 = 9, 699, 690 \text{ and } \varphi(A_8) = 1, 658, 880. \text{ Write } \]

\[ Z_{A_8} = \{1 < v_1 < v_2 < \ldots < v_{\varphi(A_8)}\}. \]

For \( r \in Z_{A_8} \), define \( h_r^{(8)} = i \) if \( r = v_i \) for some \( 1 \leq i \leq \varphi(A_8) \). Let

\[ \mathfrak{R} = \{1 \leq r < A_{10} : \gcd(A_8, r) = 1\} = \{1 = r_1 < r_2 < \ldots < r_{|\mathfrak{R}|}\}, \]

which is a set a little larger than \( Z_{A_{10}} \) and contains \( 1 \leq r < A_{10} \) with \( 23|r \) or \( 29|r \). Then \( |\mathfrak{R}| = \varphi(A_8) \cdot 23 \cdot 29 = 1, 106, 472, 960 \). For \( r \in \mathfrak{R} \) define

\[ \xi(r) = \lfloor r/A_8 \rfloor \cdot \varphi(A_8) + h_r^{(8)} \mod A_8. \]

For \( 1 \leq j \leq |\mathfrak{R}| \) define

\[ \eta(j) = \begin{cases} A_8 \cdot \lfloor (j - 1)/\varphi(A_8) \rfloor + v_{\varphi(A_8)}, & \text{if } \varphi(A_8)|j, \\ A_8 \cdot \lfloor (j - 1)/\varphi(A_8) \rfloor + v_j \mod \varphi(A_8), & \text{otherwise}. \end{cases} \]

Then for \( r \in \mathfrak{R} \) and \( 1 \leq j \leq |\mathfrak{R}| \), we have \( \eta(\xi(r)) = r \) and \( \xi(\eta(j)) = j \). Now the function \( \xi(r) \) serves for \( s = 10 \) as \( h_r \) serves for \( s \leq 9 \), and the function \( \eta(j) \) serves for \( s = 10 \) as \( u_j \) serves for \( s \leq 9 \). The differences are that, for \( s = 10 \), both \( \xi(r) \) and \( \eta(j) \) are computed instantly and frequently, and only the sets \( \{v_i\} \) and \( \{h_r^{(s)}\} \) are saved as arrays in memory, which take only

\[ (A_8 - 1) \cdot 4 + \varphi(A_8) \cdot 4 = 45, 434, 276 \]

bytes of memory. In the “Repeat ... Until” loop of Procedure 1, the “For \( j := 1 \) To \( \varphi(L) \) Do begin ... end” sub-loop is replaced by the following code:

\[
\text{For } j := 1 \text{ To } |\mathfrak{R}| \text{ Do begin}
\text{If } (H_0(j) > 0) \text{ And } (\gcd(\eta(j), 23 \cdot 29) = 1) \text{ Then Begin}
\text{Begin } r \leftarrow p \cdot \eta(j) \mod A_{10};
\text{If } H(\xi(r)) = 0 \text{ Then } t \leftarrow t + 1;
\text{H}(\xi(r)) \leftarrow H(\xi(r)) + H_0(j)
\text{End}
\text{End.}
\]

Remark 2.3. In any event, the arrays \( H(j) \) and \( H_0(j) \) (\( 1 \leq j \leq |\mathfrak{R}| \)) for \( s = 10 \) could not be saved in the memory of my PC. They are saved in disk files. Since

\[ 2^{64} < g_{10,1} = 21, 823, 464, 288, 660, 487, 575, 563, 042, 953, 246, 059 < 2^{128}, \]

it takes \( |\mathfrak{R}| \cdot 2 \cdot 128/8 \approx 36 \text{ GB disk space to store } H(j) \) and \( H_0(j) \) for \( 1 \leq j \leq |\mathfrak{R}| \). Since \( 9^{63} - 1 = 9, 223, 372, 036, 854, 775, 807 \) is the maximum integer in Delphi 6.0, a multi-precision package is needed for \( s = 10 \).
Acknowledgments

I thank Professors C. Pomerance and A. Granville for valuable comments on the original versions of this paper. Special thanks go to the referee for friendly and helpful comments that improved the presentation of this paper.

References


Department of Mathematics, Anhui Normal University, 241000 Wuhu, Anhui, People’s Republic of China

E-mail address: zhangzhx@mail.wh.ah.cn
E-mail address: ahnu_zxx@sina.com
URL: http://www.ahnu.edu.cn/site/math/htm1/zzx.htm