ON CARMICHAEL NUMBERS WITH 3 FACTORS

STEFAN KOHL

ABSTRACT. In this short note it is shown that any Carmichael number with 3 prime factors one of which is p is smaller than $2p^6$. Using this, it is found by means of computation that 1223 is the smallest odd prime which does not divide a Carmichael number with 3 factors.

1. INTRODUCTION

Let n be a positive integer. If n is prime, then for any $a \in \mathbb{N}$ which is coprime to n we have $a^{n-1} \equiv 1 \mod n$. If n is composite, this is usually not the case. Therefore testing this condition can be used as a naive pseudoprime test. Composite n which fool this test are widely known as *Carmichael numbers*.

As can be found in many elementary textbooks (see e.g. [1], Chapter III, Theorem 18), a positive integer n is a Carmichael number if and only if $n = p_1p_2 \dots p_r$ where $r \geqslant 3$ and $p_1, p_2, \dots, p_r$ are distinct odd primes which satisfy $(p_i - 1)|(n - 1),\ i = 1, 2, \dots, r$.

In this note we look at Carmichael numbers which have the least possible number 3 of factors. We show that their factors cannot differ arbitrarily much in size, and we determine the least odd prime which does not occur as a factor of a Carmichael number with 3 factors.

2. THE BOUNDS

Theorem 2.1. *Let $n = p_1p_2p_3$ be a Carmichael number with 3 prime factors. Without loss of generality, assume that $p_2 < p_3$. Then the following hold:*

(1) $p_2 < 2p_1^2$.
(2) $p_3 < p_1^3$.
(3) $n < 2p_1^6$.

Proof. Let $n = p_1p_2p_3$ be a Carmichael number with 3 factors. From above we know that $(p_i - 1)|(n - 1)$ for $i \in \{1, 2, 3\}$. We conclude that

- $(p_3 - 1)|(p_1p_2 - 1) \Rightarrow p_1p_2 - 1 = a(p_3 - 1)$ for some $a \in \mathbb{N}$, and that
- $(p_2 - 1)|(p_1p_3 - 1) \Rightarrow p_1p_3 - 1 = b(p_2 - 1)$ for some $b \in \mathbb{N}$.

The assumption $p_2 < p_3$ implies $a < b$. Further it is

- $a \geqslant 2$ since $p_1p_2 - 1 = 1(p_3 - 1)$ contradicts the primality of p_3, and
- $b \geqslant 2$ since $p_1p_3 - 1 = 1(p_2 - 1)$ contradicts the primality of p_2.

We also get

- $p_1p_2 - 1 = a(p_3 - 1) = ap_3 - a \Longrightarrow p_3 = (p_1p_2 + a - 1)/a$, and
- $p_1p_3 - 1 = b(p_2 - 1) = bp_2 - b \Longrightarrow p_2 = (p_1p_3 + b - 1)/b$.

2000 *Mathematics Subject Classification.* Primary 11A51, Secondary 11-04.

Inserting the former equation into the latter yields

$$p_2 \;=\; \frac{p_1(p_1p_2+a-1)/a+b-1}{b} \;=\; \frac{p_1^2p_2+ab+(p_1-1)a-p_1}{ab}.$$

This implies that

$$(p_1^2-ab)p_2+ab+(p_1-1)a-p_1 \;=\; 0,$$

from which we get

$$p_2 \;=\; \frac{ab+(p_1-1)a-p_1}{ab-p_1^2} \;<\; \frac{ab}{ab-p_1^2} \;+\; \frac{(p_1-1)a}{ab-p_1^2}.$$

We have $ab \neq p_1^2$, since assuming the contrary yields $a = b = p_1 \Rightarrow p_1p_2 - 1 = p_1(p_3-1) \Rightarrow p_3 = p_2 + 1 - 1/p_1 \notin \mathbb{N}$, which is not possible. Further it is $ab > p_1^2$ since $p_2 > 0$ and $ab + (p_1-1)a > 0$. This yields

$$\frac{ab}{ab-p_1^2} \;\leqslant\; \frac{p_1^2+1}{(p_1^2+1)-p_1^2} \;=\; p_1^2+1.$$

Here we use that for any positive real numbers x, y and z where $x > y > z$, we have $x/(x-z) < y/(y-z)$.

By the assumption $p_2 < p_3$ we have $p_1(p_3-1) > p_1p_2 - 1 = a(p_3-1)$, hence $a < p_1$. We conclude that

$$\frac{(p_1-1)a}{ab-p_1^2} \;<\; \frac{(p_1-1)p_1}{ab-p_1^2} \;\leqslant\; p_1^2-p_1.$$

This yields $p_2 < p_1^2 + 1 + p_1^2 - p_1 < 2p_1^2$, which is the first assertion. From $p_1p_2 - 1 = a(p_3-1)$ and $a \geqslant 2$ we get $p_3 \leqslant (p_1p_2+1)/2 < (2p_1^3+1)/2$, and therefore our second assertion $p_3 < p_1^3$ holds as well. Finally we get $n = p_1p_2p_3 < p_1 \cdot 2p_1^2 \cdot p_1^3 = 2p_1^6$, as claimed. □

3. Computational Results

The Carmichael numbers $561 = 3 \cdot 11 \cdot 17$, $10585 = 5 \cdot 29 \cdot 73$ and $52633 = 7 \cdot 73 \cdot 103$ show that the bounds $p_2 < 2p_1^2$ and $p_3 < p_1^3$ cannot be improved to $p_2 < p_1^2$ and $p_3 < p_1^3/2$, respectively. There are also larger examples for this, like $471905281 = 31 \cdot 991 \cdot 15361$, $2489462641 = 41 \cdot 1721 \cdot 35281$ and $167385219121 = 83 \cdot 6971 \cdot 289297$.

Next we look at the question which primes divide how many Carmichael numbers with three factors. The following table has been obtained by a GAP [2] program which is based on Theorem 2.1:

k	Primes $p < 2000$ which divide k Carmichael numbers with 3 factors
0	1223 1487
1	3 11 59 197 389 467 479 503 563 719 839 887 1523 1907
2	23 79 83 149 167 233 283 317 347 359 643 653 773 907 1103 1109 1367 1439 1459 1493 1553 1787 1823 1847 1949
3	5 47 53 107 173 383 419 499 557 1019 1031 1049 1091 1187 1259 1511 1559 1579 1637 1699 1889
4	19 29 67 101 179 227 263 269 509 587 593 677 821 857 947 983 1033 1063 1097 1129 1217 1229 1279 1289 1319 1427 1481 1619 1697
5	17 89 137 223 239 293 463 647 739 743 769 863 881 929 1151 1291
	To be continued.

Continued.	
k	Primes $p < 2000$ which divide k Carmichael numbers with 3 factors
	1373 1543 1549 1709 1733 1747 1811 1867 1877 1931 1979 1997
6	7 103 113 139 191 257 349 431 439 449 569 599 683 709 809 827 977 1039 1163 1181 1447 1451 1567 1583 1627 1777 1879 1913
7	71 229 461 659 787 797 971 1123 1193 1231 1307 1409 1423 1433 1613 1753 1759 1973
8	13 37 97 127 163 251 353 373 443 521 523 691 853 859 1087 1283 1483 1499 1871 1933
9	31 41 199 277 311 367 619 641 829 1021 1277 1361 1601 1663 1667 1669 1721 1999
10	281 397 409 491 607 877 941 967 1061 1249 1399 1571 1597 1607 1693 1783
11	73 131 151 193 457 823 919 1237
12	43 109 307 379 487 727 757 761 937 953 997 1069 1213 1453 1609 1741 1873 1901 1951 1993
13	571 733 751 883 1013 1381 1429 1471 1723 1831
14	157 401 547 617 911 1009 1117 1303 1489
15	181 241 811 1201 1301 1789 1987
16	61 601 631 673
17	433 577 613 1051 1093 1153 1327 1861
18	701 1621
19	337 1531
20	313 331 541 661 991 1801
21	271
22	211
23	1297 1321
24	421 1657
25	1171

In particular we observe that the smallest odd prime which does not divide a Carmichael number with three factors is 1223.

REFERENCES

1. Harald Scheid, *Zahlentheorie*, BI-Wissenschaftsverlag, 1991.
2. The GAP Group, *GAP – Groups, Algorithms, and Programming; Version 4.4.9*, 2006, http://www.gap-system.org.

INSTITUT FÜR GEOMETRIE UND TOPOLOGIE, PFAFFENWALDRING 57, UNIVERSITÄT STUTTGART 70550 STUTTGART, GERMANY
E-mail address: kohl@mathematik.uni-stuttgart.de