Carmichael Numbers

1. Introduction

Consider the following well-known theorem:

Theorem (Fermat's Little Theorem): Let p be a prime. For all $a \equiv 0 \pmod{p}$, we have

$$a^{p-1} \equiv 1 \pmod{p}.$$

What happens if we assume that p isn't prime? If p isn't prime but satisfies the theorem above, then p is called a *Carmichael number*. In this paper, we will be exploring Carmichael numbers, some of their properties, and most importantly, how they are distributed.

2. Basics

Let's define what a Carmichael number is again.

Definition (Carmichael Number): A composite integer n is called a *Carmichael number* if for all a such that $\gcd(a, n) = 1$ we have

$$a^{p-1} \equiv 1 \pmod{p}.$$

Example: Here are a few examples of Carmichael numbers:

$$561, 1105, 1729$$

Clearly going through every single possible a and checking the condition above would be an inneficient way to determine if a number is a Carmichael number or not. The following criterion gives a much faster way to find out.

Theorem (Korselt's Criterion): A composite number n is a Carmichael number if and only if
- n is squarefree,
- for every prime p dividing n, we also have $(p-1) \mid (n-1)$.

Proof: Assume n is a Carmichael number. We will first show that n is squarefree via contradiction. Suppose some prime p divides n more than once. Thus we can write $n = p^k n'$ where $k = \nu_p(n) \geq 2$. By the Chinese Remainder Theorem, there exists a such that

$$a \equiv 1 + p \left(\operatorname{mod} p^k\right) \quad \text{and} \quad a \equiv 1 \left(\operatorname{mod} n'\right).$$

These two equations imply that $\gcd(a, n) = 1$, so by the definition of Carmichael numbers we have

$$a^{n-1} \equiv 1 \left(\operatorname{mod} n\right).$$

This means $a^{n-1} - 1 = nm$ for some integer m. Taking both sides $\operatorname{mod} p^2$ yields

$$(1+p)^{n-1} \equiv 1 \left(\operatorname{mod} p^2\right).$$

Using the binomial theorem on the left side gets rid of all terms except the first two, so we have

$$1 + (n-1)p \equiv 1 \left(\operatorname{mod} p^2\right).$$

Since p^2 divides n, we have

$$1 - p \equiv 1 \left(\operatorname{mod} p^2\right),$$

which is impossible, so n must be squarefree.

Next we show $(p-1) \mid (n-1)$ for each prime $p \mid n$. Since n is squarefree, p and $\frac{n}{p}$ are relatively prime. Pick any b such that b is a primitive root of p. By the Chinese Remainder Theorem, there exists an a such that

$$a \equiv b \left(\operatorname{mod} p\right) \quad \text{and} \quad a \equiv 1 \left(\operatorname{mod} \frac{n}{p}\right).$$

These two equations imply $\gcd(a, n) = 1$, so we have

$$a^{n-1} \equiv 1 \left(\operatorname{mod} n\right).$$

Reducing mod p yields

$$b^{n-1} \equiv 1 \left(\operatorname{mod} p\right).$$

Since $\operatorname{ord}_p(b) = p - 1$, we must have $(p-1) \mid (n-1)$.

Now we show the other direction. Assume n composite, squarefree, and $(p-1) \mid (n-1)$ for all primes p dividing n. If $\gcd(a, n) = 1$, then for each prime $p \mid n$ we have $\gcd(a, p) = 1$, so

$$a^{p-1} \equiv 1 \left(\operatorname{mod} p\right).$$

Since $p - 1$ is a factor of $n - 1$, we have

$$a^{n-1} \equiv 1 \left(\operatorname{mod} p\right).$$

Since this holds for all primes dividing n, we can deduce

$$a^{n-1} \equiv 1 \pmod{n},$$

so n is a Carmichael number. ∎

Here is a way to construct Carmichael numbers.

Example: Let $n = (6k+1)(12k+1)(18k+1)$ where $k \geq 1$. Suppose k is chosen such that $6k+1, 12k+1$, and $18k+1$ are all prime. First it's clear that n is squarefree. Now exapand n to get

$$n = 1296k^3 + 396k^2 + 36k + 1.$$

Note that we have $6k \mid (n-1)$, $12k \mid (n-1)$, and $18k \mid (n-1)$. Thus n satisfies Korselt's criterion, so it is Carmichael number. Similarly, if k is chosen such that $6k+1, 12k+1, 18k+1,$ and $36k+1$ are all primes, then $n = n = (6k+1)(12k+1)(18k+1)(36k+1)$ is a Carmichael number. However, not every Carmichael number is of one of these forms. For example, $561 = 3 \cdot 11 \cdot 17$, which does not fall into one of these categories.

Next we deduce some properties that Carmichael numbers must have.

Proposition: Every Carmichael number n is odd, has at least three different prime factors, and every prime factor of n is less than $\sqrt{n}$.

Proof: Suppose n is even. Then by Korselt's Criterion we need $(p-1) \mid (n-1)$ for all primes dividing n. However, if p is an odd prime, then $p-1$ is even, while $n-1$ is odd, which means $(p-1) \mid (n-1)$ can't hold. Thus, n must be odd.

Now suppose $n = pq$ has two prime factors. By Korselt's Criterion, we have $(p-1) \mid (pq-1)$. This implies

$$\frac{pq-1}{p-1}$$

is an integer. We can rewrite this as

$$\frac{pq - q + q - 1}{p-1} = q + \frac{q-1}{p-1}.$$

Thus we need $(p-1) \mid (q-1)$. Using the same process, we also have $(q-1) \mid (p-1)$. Both of these imply $p - 1 = q - 1$, but this is impossible. Thus, n must have at least three prime factors.

Now we show that every prime factor is less than $\sqrt{n}$. If p is a prime factor, then we have

$$\frac{n-1}{p-1} = \frac{p\left(\frac{n}{p}\right) - 1}{p-1} = \frac{(p-1)\left(\frac{n}{p}\right) + \frac{n}{p} - 1}{p-1} = \frac{n}{p} + \frac{\frac{n}{p} - 1}{p-1},$$

so $(p-1) \mid \left(\frac{n}{p} - 1\right)$. Thus $p \leq \frac{n}{p}$. Note that is the inequality is not strict then $n = p^2$, which is impossible. Thus we obtain $p < \sqrt{n}$, as desired. ∎

[1]

3. Distribution

Now we'll discuss the distribution of Carmichael numbers. The first obvious question we should ask: are there infinitely many Carmichael numbers? The answer is yes.

Theorem (Alford, Granville, Pomerance): Let $C(x)$ denote the number of Carmichael numbers up to x. Then

$$C(x) > x^{\frac{2}{7}}$$

for sufficiently large x.

The proof of this theorem is quite involved, so we won't delve into it here, but a full proof can be found at [2].

Another reasonable question that can be asked is how many Carmichael numbers with k factors are there? Letting $C_k(x)$ denoting the number of Carmichael numbers up to x with exactly k prime factors, Granville conjectured that

$$C_k(x) = x^{\frac{1}{k}+o_k(x)}.$$

In fact, we can get a bound on $C_3(x)$ that is quite close to this value.

Theorem (Balasubrmanian, Nagaraj): Let $C_3(x)$ denote the number of Carmichael numbers up to x with exactly 3 prime factors. Then

$$C_3(x) = x^{\frac{5}{14}+o(1)}$$

for sufficiently large x.

Proof: Let n be a Carmichael number with three prime factors $2 < p < q < r$. By Korselt's Criterion, we have

$$n - 1 \equiv 0 \pmod{p-1},$$
$$n - 1 \equiv 0 \pmod{q-1},$$
$$n - 1 \equiv 0 \pmod{r-1}.$$

Let $g = \gcd(p-1, q-1, r-1)$. Define a, b, c as $\frac{p-1}{g}, \frac{q-1}{g}, \frac{r-1}{g}$ respectively. Thus $a < b < c$. Note that $n - 1 \equiv 0 \pmod{p-1} \Rightarrow n - 1 \equiv 0 \pmod{ga} \Rightarrow n - 1 \equiv 0 \pmod{a}$. Writing the left side in terms of g, a, b, c yields

$$(ga+1)(gb+1)(gc+1) - 1 \equiv (gb+1)(gc+1) - 1 = g(gbc+b+c) \equiv 0 \pmod{a}.$$

This implies $gbc + b + c \equiv 0 \pmod{a}$. Similarly, $gab + a + b \equiv 0 \pmod{c}$ and $gac + a + c \pmod{b}$. Combining these using Chinese Remainder Theomrem yields

$$g(ab + bc + ca) + a + b + c \equiv 0 \pmod{abc}.$$

Note that $\gcd(ab + bc + ca, abc) = 1$. Thus, given a, b, c, g is uniquely determined mod abc.

Let N be the number of quadruples (g, a, b, c) that satisfy the above congruence and such that $g^3 abc \leq x$. Then $C_3(x) \leq N$. We write $N = N_1 + N_2 + N_3$ where N_1 is the number of quadruples with $g > abc$, N_2 is the number of quadruples with $G < g \leq abc$ where $G = x^{\frac{3}{14}}$, and N_3 is the number of quadruples with $g \leq G$ and $g \leq abc$.

First we estimate N_1. If (a, b, c) is fixed, then the number of g with $g^3 abc \leq x$ that are in particular residue class mod abc is at most $\left(\frac{x}{abc}\right)^{\frac{1}{3}} / (abc) = \frac{x^{\frac{1}{3}}}{(abc)^{\frac{4}{3}}}$. Thus we have

$$N_1 = \sum_{a<b<c} \frac{x^{\frac{1}{3}}}{(abc)^{\frac{4}{3}}} < \frac{\zeta\left(\frac{4}{3}\right)^3 x^{\frac{1}{3}}}{6}.$$

The cubed ζ comes from considering just summing over one variable and then multiplying each sum together, and the division by 6 comes from considering permutations. Thus $N_1 = O\left(x^{\frac{1}{3}}\right)$.

Next we estimate N_2. If (a, b, c) is fixed, then there is at most one g that satisfies our congruence and that is less than abc. If $g > G$ and $g^3 abc \leq x$, then $abc \leq \frac{x}{g^3} < \frac{x}{G^3}$. Thus N_2 is at most the number of triples (a, b, c) with $a < b < c$ and $abc \leq \frac{x}{G^3}$. Note that a can be at most $\left(\frac{x}{G^3}\right)^{\frac{1}{3}}$ under these conditions, b is at most $\left(\frac{x}{aG^3}\right)^{\frac{1}{2}}$, and c is at most $\frac{x}{abG^3}$. Thus we have

$$\begin{aligned} N_2 &\leq \sum_{1 \leq a < \frac{x^{\frac{1}{3}}}{G}} \sum_{a < b < \left(\frac{x}{aG^3}\right)^{\frac{1}{2}}} \sum_{b < c \leq \frac{x}{abG^3}} 1 \\ &< \sum_{1 \leq a < \frac{x^{\frac{1}{3}}}{G}} \sum_{a < b < \left(\frac{x}{aG^3}\right)^{\frac{1}{2}}} \frac{x}{abG^3} < \sum_{1 \leq a < \frac{x^{\frac{1}{3}}}{G}} \left(\frac{x}{aG^3}\right) \log\left(\left(\frac{x}{aG^3}\right)^{\frac{1}{2}}\right) \\ &< \frac{x}{2G^3}\left(1 + \log\left(\frac{x^{\frac{1}{3}}}{G}\right)\right) \log\left(\frac{x}{G^3}\right) < \frac{x}{6G^3} \log^2 x = \frac{1}{6} x^{\frac{5}{14}} \log^2 x. \end{aligned}$$

Thus $N_2 = O\left(x^{\frac{5}{14} + o(1)}\right)$.

Finally we estimate N_3. Finding the estimate for N_3 is much more involved, so if the reader is interested in reading the proof in its entirety, we leave a leave reference to the original paper [3]. However, we will outline the beginning of the estimate. In this case $g \leq G$ and $g \leq abc$ where $G = x^{\frac{3}{14}}$. Let $g(ab + bc + ca) + a + b + c = \lambda abc$ where λ is a positive integer. Then

$$(\lambda a - g) bc = ga(b + c) + a + b + c.$$

Note that $6gbc \geq g(ab + bc + ca) + a + b + c = \lambda abc$, so $\lambda a \leq 6g$. We break the range for g, a, b as $G_1 \leq g \leq 2G_1$, $A \leq a \leq 2A$, $B \leq b \leq 2B$. We consider two cases: $B \geq Ax^{\frac{1}{14}}$ and $B < Ax^{\frac{1}{14}}$. From there the paper considers both cases separately, and both have $O\left(x^{\frac{5}{14} + o(1)}\right)$ choices for λ, g, a, b, c.

Thus, overall we have

$$N = N_1 + N_2 + N_3 = O\left(x^{\frac{1}{3}}\right) + O\left(x^{\frac{5}{14} + o(1)}\right) + O\left(x^{\frac{5}{14} + o(1)}\right) = O\left(x^{\frac{5}{14} + o(1)}\right),$$

as desired. ■

References

[1] K. Conrad, “Carmichael Numbers and Korselt’s Criterion,” *Available at: carmichaelkorselt. pdf (Accessed 2 June 2022)*, 2016.

[2] W. R. Alford, A. Granville, and C. Pomerance, “There are infinitely many Carmichael numbers,” *Annals of Mathematics* , vol. 139, no. 3, pp. 703–722, 1994.

[3] R. Balasubramanian and S. Nagaraj, “Density of Carmichael numbers with three prime factors,” *Mathematics of computation* , vol. 66, no. 220, pp. 1705–1708, 1997.