CARMICHAEL NUMBERS

ALEX THOLEN

Definition 1. A Carmichael number n is a non-prime where for all a, we get that $a^n \equiv a \mod n$.

Non-prime is necessary, as this condition is satisfied by all primes, due to Fermat's Little Theorem. The existence of Carmichael numbers are a counterexample to the converse of Fermat's Little Theorem - as the theorem states that primes satisfy $a^n \equiv a \mod n$ for all a, and Carmichael numbers aren't prime. The first Carmichael numbers were found in 1910, but not until 1992, when the source I used published, was it known that there was an infinite amount of them.

Definition 2. Euler's totient function denoted by $\phi(n)$ is the number of numbers relatively prime to n up to n.

For example, $\phi(1) = 1, \phi(2) = 1, \phi(3) = 2, \phi(4) = 2, \phi(10632) = 3536 \dots$

Definition 3. Let $C(x)$ be the number of Carmichael numbers up to x.

Other people have proven that $C(x) \leq x^{1-(1+o(1)) \log\log\log x / \log\log x}$, however that isn't relevant to proving infinitude.

Definition 4. Let $\pi(x)$ be the number of primes $p \leq x$, and let $\pi(x, y)$ be the number of these for which $p - 1$ is free of prime factors exceeding y. Let $\pi(x; d, a)$ be the number of primes up to X that are a mod d.

The prime number theorem says that that is roughly $\frac{\pi(x)}{\phi(d)}$.

Definition 5. Let $\mathcal{E}$ be the set of numbers E in the range $0 < E < 1$ for which there are numbers $x_1(E), y_1(E) > 0$ such that $\pi(x, x^{1-E}) \geq y_1(E)\pi(x)$ for all $x \geq x_1(E)$.

It has been proven in the past that any positive number less than $1 - (2\sqrt{e})^{-1} \approx 0.7$ is in $\mathcal{E}$, but to prove infinitude, it suffices to show that some positive number is in $\mathcal{E}$. We will not be proving it, however. Erdős conjectured that all numbers less than 1 are in $\mathcal{E}$.

Definition 6. Let $\mathcal{B}$ denote the set of numbers B in the range $0 < B < 1$ for which there is a number $x_2(B)$ and a positive integer D_B, such that for each $x \geq x_2$, there is a set $D_B(x)$ of at most D_B integers, each exceeding $\log(x)$, with

$$\pi(y; d, a) \geq \frac{\pi(y)}{2\phi(d)}$$

whenever $(a, d) = 1, 1 \leq d \leq \min\{x^B, \frac{y}{x^{1-B}}\}$and d is not divisible by any members of D_B.

Theorem 7. *Korselt's criterion: n is a Carmichael number if and only if n is squarefree and $p - 1$ divides $n - 1$ for all primes p dividing n.*

Date: June 17, 2019.

Proof. Squarefree is obvious: If it isn't squarefree, then a number whose square is a factor of n can not return to itself mod n. To prove the fact that $p-1$ divides $n-1$ for all primes p dividing n, you have to look at Euler's extension to Fermat's Little Theorem, which states that for all a relatively prime to n, $a^{\phi(n)+1} - a \equiv 0 \mod n$. One fact about modulo is that there is always a primitive root. A primitive root is a number where $r^{\pi(n)} = 1$, and for no positive smaller such exponent is the same true. Look at those primitive roots to the nth power. That result must be 1, due to the definition of Carmichael number, and so $\phi(n) \mid n-1$. Since $\phi(n) = (p_1-1)(p_2-1)(p_3-1)\cdots$, we obtain this criterion. This is also sufficient, due to the fact that if this works then there could be no such a otherwise. ■

Definition 8. The group ring $R[G]$ where R is a ring and G is a group is the set of mappings $f : G \to R$ where there are only finitely many nonzero outputs. We define elements as expressions of the form $r_1g_1 + \cdots + r_ng_n$, and addition is defined as $(r_1g_1 + \cdots + r_ng_n) + (s_1g_1 + \cdots + s_ng_n) = (r_1+s_1)g_1 + \cdots + (r_n+s_n)g_n$ with multiplication being defined as $(r_1g_1 + \cdots + r_ng_n)(s_1g_1 + \cdots + s_ng_n) = \sum_{i=1}^n \sum_{j=1}^n r_is_jg_{ij}$.

Definition 9. Carmichael's lambda function is defined as $\lambda(p^a) = \phi(p^a)$ for $p \neq 2$. For $a \geq 3$, $\lambda(2^a) = \frac{1}{2}\phi(2^a)$. For $a = 0, 1, 2$ we get that $\lambda(2^a) = \phi(2^a)$. And for $n = p_1^{a_1}p_2^{a_2}p_3^{a_3}\cdots p_k^{a_k}$ we get that $\lambda(n) = \lambda(p_1^{a_1})\lambda(p_2^{a_2})\lambda(p_3^{a_3})\cdots\lambda(p_k^{a_k})$.

Definition 10. $n(G)$ is the length of the longest sequence of (not necessarily distinct) members of G such that no subsequence of non-zero length has a product of the identity.

Theorem 11. *If G is a finite abelian group and m is the maximal order of an element in G, then $n(G) < m\left(1 + \log\left(\frac{|G|}{m}\right)\right)$.*

Proof. Let $g_1, g_2, \ldots, g_n$ be a sequence of elements of G and assume $n \geq m\left(1 + \log\left(\frac{|G|}{m}\right)\right)$. Choose q to be any prime with $q \equiv 1 \mod m$ and let $\mathbf{F}_q$ denote the field of q elements. If we multiply out the product

$$(a_1 - g_1)(a_2 - g_2)\ldots(a_n - g_n) = \sum_{g\in G} k_g g$$

in the group ring $\mathbf{F}_q[G]$ where $a_1, a_2, \ldots a_n$ are nonzero elements of $\mathbf{F}_q$ and suppose that no subsequence of $g_1, g_2, \ldots, g_n$ has product equal to 1, then $k_1 = a_1a_2\ldots a_n$. Thus if we can find $a_1, a_2, cd\cdots, a_n$ such that the product is 0, we have a contradiction. We can turn a character χ of the form $G \to \mathbf{F}_q/\{0\}$ into a ring homomorphism $x : \mathbf{F}_q[G] \to \mathbf{F}_q$ by letting $x(\sum_{g\in G} k_g g) = \sum_{g\in G} k_g\chi(g)$. From the orthogonality relations for group characters, we can see that if $b \in \mathbb{F}_q[G]$ then $b = 0$ iff $\chi(b) = 0$ for all $\chi \in G$. Thus, since $\chi(\prod_{i=1}^n (a_i - g_i)) = \prod_{i=1}^n (a_i - \chi(g_i))$, we can see that the product is 0 if for each $\chi \in G$ there exists $1 \leq j \leq n$ such that $\chi(g_j) = a_j$. So, we need to select $a_1, a_2, a_3\cdots a_n$ so that for each character we can find some such j. Since G is finite, it is possible to pick such an a_1 to maximize the number of characters in G where $\chi(g+1) = a_1$. Pick a_2 such that $\chi(g_2) = a_2$ for as many of the remaining $\chi \in G$ as possible, and so on. Each $\chi(g_j)$ is an mth root of 1 in $\mathbf{F}_q$, and so can be one of only m different values. Thus, if S is any subset of G and g is any element of G, then there is some nonzero $a \in \mathbf{F}_q$ with $\chi(g) = a$ holding for at least $\frac{|S|}{m}$ characters $\chi \in S$. That means that $\chi(g) = a$ does not hold for at most $|S|(1 - \frac{1}{m})$ characters $\chi \in S$. Doing this picking method for $g_1, g_2, \cdots, g_k$ where $k = \lfloor m\log(\frac{|G|}{m})\rfloor + 1$ will allow us to choose

$a_1, a_2, \cdots, a_k \in \mathbf{F}_q$ such that the set of the characters where $\chi(g) = 1$ does not hold has cardinality of at most

$$|G|(1 - \frac{1}{m})^k < |G|e^{-\frac{k}{m}} < m$$

Since $n \geq k + m - 1$, we have enough remaining a_i such that we can individually pick of the remaining characters. Henceforth we have a contradiction. Q.E.D. ■

Theorem 12. *Suppose that B is in the set $\mathcal{B}$. There exists a number $x_3(B)$ such that if $x \geq x_3(B)$ and L is a squarefree integer not divisible by any prime exceeding $x^{\frac{(1-B)}{2}}$ and for which $\sum_{primeq|L} \frac{1}{q} \leq \frac{(1-B)}{32}$, then there is a positive integer $k \leq x^{1-B}$ with $(k, L) = 1$, such that*

$$\#\{d \mid L : dk + 1 \leq x, dk + 1 \text{ is prime}\} \geq \frac{2^{-D_b - 2}}{\log x} \#\{d \mid L : 1 \leq d \leq x^B\}$$

Proof. We let $x_3(B) = \max\{x_2(B), 17^{\frac{1}{1-B}}\}$. Suppose that B, x and L satisfy the hypotheses. For each $d \in \mathcal{D}_B(x)$ with $(L, d) > 1$, remove some prime factor of (L, d) from L, so as to obtain a number L' which is not divisible by any member of $\mathcal{D}_B(x)$. Therefore $\omega(L') \geq \omega(L) - \mathcal{D}_B$, where $\omega(m)$ is the number of prime divisors of m. For each divisor d of L with $1 \leq d \leq y$, the integer $d' = \frac{d}{(d, \frac{L}{L'})}$ is a divisor of L' in. the range $1 \leq d' \leq y$. Further, there are at most $2^{\omega(\frac{L}{L'})} \leq 2^{\mathcal{D}_B}$ different values of d which map to the same number d'. That means that

$$\#\{d \mid L' : 1 \leq d \leq y\} \geq 2^{-\mathcal{D}_B} \#\{d \mid L : 1 \leq d \leq y\}$$

for any $y \geq 1$. From the definition of B, we can see that for each divisor d of L' with $1 \leq d \leq x^B$ we have

$$\pi(dx^{1-B}; d, 1) \geq \frac{\pi(dx^{1-B})}{2\phi(d)} \geq \frac{dx^{1-B}}{2\phi(d)\log(dx^{1-B})} \geq \frac{dx^{1-B}}{2\phi(d)\log x}$$

since $\pi(y) \geq \frac{y}{\log y}$ for all $y \geq 17$. Our hypotheses stated that any prime factor q of L is at most $x^{\frac{(1-B)}{2}}$, and so we can use that $\pi(x; q, a) \leq \frac{2x}{\varphi(q)\log(x/q)}$ (due to the Brun-Titchmarsh theorem) to get

$$\pi(dx^{1-B}; d, 1) \geq \frac{\pi(dx^{1-B})}{\phi(dq)\log(\frac{x^{1-B}}{q})} \geq \frac{4}{\phi(q)(1-B)} \frac{dx^{1-B}}{\phi(d)\log x} \leq \frac{8}{q(1-B)} \frac{dx^{1-B}}{\phi(d)\log x}$$

Therefore if we combine the two, we get that the number of primes $p \leq dx^{1-B}$ with $p \equiv 1 \mod d$ and $(\frac{(p-1)}{d}, L) = 1$ is at least

$$\pi(dx^{1-B}; d, 1) - \sum_{\text{prime } q|L} \pi(dx^{1-B}; dq, 1) \geq \left(\frac{1}{2} - \frac{8}{1-B} \sum_{\text{prime} q|L} \frac{1}{2}\right) \frac{dx^{1-B}}{\phi(d)\log x} \geq \frac{x^{1-B}}{4\log x}.$$

Thus we have at least

$$\frac{x^{1-B}}{5\log x} \#\{d \mid L' : 1 \leq d \leq x^B\}$$

pairs (p, d) where $p \leq dx^{1-B}$ is prime, $p \equiv 1 \mod d$, $(\frac{p-1}{d}, L) = 1$, $d \mid L'$ and $1 \leq d \leq x^B$. Each such pair (p, d) corresponds to an integer $\frac{(p-1)}{d} \leq x^{1-B}$ that is coprime to L, and so there is at least one integer $k \le x^{1-B}$ with $(k, L) = 1$ such that k has at least

$$\frac{1}{4\log x}\#\{d \mid L' : 1 \le d \le x^B\}$$

representations as $\frac{(p-1)}{d}$ with (p, d) as above. Thus for this integer k we have

$$\#\{d \mid L : dk+1 \le x, dk+1 \text{ is prime}\} \ge \frac{1}{4\log x}\#\{d \mid L' : 1 \le d \le x^B\}.$$

Combining this and our first equation gets us our desired equation. ■

Proposition 13. *Let G be a finite abelian group and let $r > t > n = n(G)$ be integers. Then any sequence of r elements of G contains at least $\frac{\binom{r}{t}}{\binom{r}{n}}$ distinct subsequences of length at most t and at least $t-n$ whose product is the identity.*

Proof. Let R be a sequence of r elements of G. Since $r > n$, there is, by the definition of $n(G)$, some subsequence of r whose product is 1. Let S be the longest such subsequence with length s. Then $s \ge r-n$, since otherwise $R\backslash S$ contains a subsequence whose product is 1, and this subsequence might be appended to S, increasing its size, which is a contradiction. Let T be any subsequence of S of size $t-n$. If the product of the elements of T is g, then the product of the elements of $S\backslash T$ is g^{-1}. Let U be smallest (possibly empty) subsequence of $S\backslash T$ whose product is G^{-1}. Evidently U has size at most n, else, by hypothesis, there exists a subsequence of U that has product 1 and this can be removed from U to make it smaller. Look at $T \cup U = V$. This is a subsequence of S and thus also R in which the product of the elements is 1, and has size at most $t-n+n = t$, and at least $t-n$. The number of ways of choosing such a pair of sequences (T, U) is at least the number of ways of choosing T and is thus at least $\binom{s}{t-n}$. The maximum possible number of different sequences T which give rise to the same sequence $V = T \cup U$ is at most $\binom{|V|}{t-n} \le \binom{t}{t-n} = \binom{t}{n}$. That means that the number of different subsequences V that we have created is at least

$$\frac{\binom{s}{t-n}}{\binom{t}{n}} \ge \frac{\binom{r-n}{t-n}}{\binom{t}{n}} = \frac{\binom{r}{t}}{\binom{r}{t}}$$

Q.E.D. ■

Theorem 14. *For each $E \in \mathcal{E}$ and $B \in \mathcal{B}$ and $\epsilon > 0$, there is a number $x_0(E, B, \epsilon)$ such that $C(x) \ge x^{EB-\epsilon}$ for all $x \ge x_0(E, B, \epsilon)$.*

Proof. Let $E \in \mathcal{E}$, $B \in \mathcal{B}$, $\epsilon > 0$. Clearly we may assume that $\epsilon < EB$. Let $\theta = \frac{1}{(1-E)}$ and let $y \ge 2$ be a parameter. Let $\mathcal{Q}$ denote the set of primes q in the range $\left(\frac{y^\theta}{\log y}, y^\theta\right]$ where $q-1$ has no prime factors bigger than y. Due to the definition of $\mathcal{E}$, for all sufficiently large y we know that

$$|\mathcal{Q}| \ge \frac{1}{2}y_1(E)\frac{y^\theta}{\log y^\theta}$$

Let L be the product of the primes $q \in \mathcal{Q}$. We know that

$$\log L \le |Q|\log(y^\theta) \le \pi(y^\theta)\log(y^\theta) \le 2y^\theta$$

again, for all large y. Now $\lambda(L)$ is the least common multiples of the numbers $q-1$, for the primes q that divide L. Since each such $q-1$ is free of prime factors exceeding y, we know that if p^α divides $\lambda(L)$, then $p \le y$ and $p^\alpha \le y^\theta$. If we let the sequence a_p be defined such that p^{a_p} is the largest power of p with $p^{a_p} \le y^\theta$, then

$$\lambda(L) \le \prod_{p \le y} p^{a_p} \le \prod_{p \le y} y^\theta = y^{\theta\pi(y)} \le e^{2\theta y}$$

for all large y. Let G be the subgroup of $(\mathbb{Z}/L\mathbb{Z})$ which is multiplicative and uses all of the relatively prime numbers. Combining both equations and Theorem 11 we get that

$$n(G) < \lambda(L)\left(1 + \log \frac{\phi(L)}{\lambda(L)}\right) \le \lambda(L)(1 + \log L) \le e^{3\theta y}$$

for all large y. Let $\sigma = \frac{\epsilon\theta}{4B}$ and let $x = e^{y^{1+\sigma}}$. Since

$$\sum_{\text{prime} q \mid L} \frac{1}{q} \le \sum_{\frac{y^\theta}{\log y} < q < y^\theta} \frac{1}{q} \le 2\frac{\log\log y}{\theta \log y} \le \frac{1-B}{32}$$

for large enough y, we can apply Theorem 12 with B, x, L. That means for all large enough y there is an integer k coprime to l that satisfies

$$|\mathcal{P}| \ge \frac{2^{-D_B-2}}{\log x}\#\{d \mid L : 1 \le d \le x^B\}$$

with $\mathcal{P}$ being the set of primes $p \le x$ with $p = dk+1$ for some divisor d of L.The product of any

$$u := \left[\frac{\log(x^B)}{\log(y^\theta)}\right] = \left[\frac{B\log x}{\theta \log y}\right]$$

distinct prime factors of L is a divisor d of L with $d \le x^B$. We deduce from the statement regarding to the size of $\mathcal{Q}$ that

$$\#\{d \mid L : 1 \le d \le x^B\} \ge \binom{\omega(L)}{u} \ge \left(\frac{\omega(L)}{u}\right)^u = ge\left(\frac{\gamma_1(E)y^\theta}{2B\log x}\right)^u = \left(\frac{\gamma_1(E)}{2B}y^{\theta-1-\gamma}\right)^u.$$

Thus, with the identity $(\theta - 1 - \gamma)\frac{B}{\theta} = EB - \frac{\epsilon}{4}$ we get that

$$|P| \ge \frac{2^{-D_B-2}}{\log x}\left(\frac{\gamma_1(E)}{2B}y^{\theta-1-\gamma}\right)^{\left[\frac{B\log x}{\theta\log x}\right]} \ge x^{EB-\frac{\epsilon}{3}}$$

for all sufficiently large values of y. Let $\mathcal{P}' = \mathcal{P}\backslash\mathcal{Q}$. Since $|\mathcal{Q}| \le y^\theta$, we have that

$$|\mathcal{P}'| \ge x^{EB-\frac{\epsilon}{2}}$$

for all sufficiently large values of y.

We can consider $\mathcal{P}'$ as a subset of the group $G = (\mathbb{Z}/L\mathbb{Z})^*$ by considering the residue class of each $p \in \mathcal{P}' \mod L$. If S is a subset of $\mathcal{P}'$ that contains more than one element and if

$$\Pi(S) := \prod_{p \in S} p \equiv 1 \mod L$$

then $\Pi(S)$ is a Carmichael number. Every member of P' is $1 \mod k$ so that $\Pi(S) \equiv 1 \mod k$, and thus $\Pi(S) \equiv 1 \mod kL$, since $\gcd(k, L) = 1$. However, if $p \in \mathcal{P}'$, then $p \in \mathcal{P}$ so that $p-1$ divides kL. So, $\pi(S)$ satisfies Korselt's criterion.

Let $t = e^{y^{1+\frac{\sigma}{2}}}$. Then, by Proposition 13, we see that the number of Carmichael numbers of the form $\Pi(S)$ where $S \subset \mathcal{P}'$ and $|S| \le t$, is at least

$$\frac{\binom{|\mathcal{P}'|}{[t]}}{\binom{|\mathcal{P}'|}{n(G)}} \geq \frac{\binom{|\mathcal{P}'|}{[t]}^{[t]}}{|\mathcal{P}'|^{n(G)}} \geq \left(x^{EB-\frac{\epsilon}{2}}\right)^{[t]-n(G)} [t]^{-[t]} \geq x^{t(EB-\epsilon)}$$

for all sufficiently large values of y using various conclusions above. Since each such number $\prod(x)$ is formed so that $\prod(S) \leq x^t$, we have that for $X = x^t$ that $C(X) \geq X^{EB-\epsilon}$ for all sufficiently large y. But $X = \exp(y^{1+\sigma}\exp(y^{1+\frac{\sigma}{2}}))$, so that$C(X) \geq X^{EB-\epsilon}$ for all sufficiently large values of X. Since y can be uniquely determined from X, this completes the proof. Q.E.D. ■

References:

Alford, W R, et al. `https://dms.umontreal.ca/~andrew/PDF/carmichael.pdf`