Generating Carmichael Numbers

Abraham Wang

Euler Circle

July 10, 2025

Introduction

What are Carmichael Numbers?

Fermat's Little Theorem

If a number p is prime, then all integers $a \in \mathbb{Z}$ such that $(a, p) = 1$ satisfy the congruence relation: $a^{p-1} \equiv 1 \mod p$.

However, is the converse also true? Unfortunately (or fortunately), it was found that there were indeed composite numbers that satisfied Fermat's little theorem.

Definition and Applications of Carmichael Numbers

Definition

A number n is Carmichael if it is composite and satisfies the congruence relation: $a^{n-1} \equiv 1 \mod n$.

Because these numbers satisfy this congruence, they can seem indistinguishable from prime numbers. These can be especially useful in primality testing; as a result, have some applications in cryptography.

Korselt's Criterion

Theorem

A number $n > 2$ is Carmichael if and only if n is squarefree and $(p-1)|(n-1)$ for all primes p dividing n.

Example

One Carmichael Number is 561. To test this case, we can see that $561 = 3 * 11 * 17$. Since 560 is divisible by $3-1, 11-1, 17-1$, then 561 is a Carmichael number.

Corrolary that follows

Corollary

For a carmichael number with only three prime factors p, q, r, then $(r-1)|(pq-1)$.

Proof.

By Korselt's Criterion, $pqr-1$ is divisible by $r-1$. We can rewrite $pqr-1 = pqr - pq + pq - 1 = pq(r-1) + (pq-1)$. Obviously, $pq(r-1)$ is divisible by $r-1$, and that means so must $pq-1$. ∎

More properties of Carmichael numbers

Proposition

All Carmichael numbers are odd.

Proof.

Since $a^{n-1} \equiv 1 \mod n$ for all a that is coprime to n, then we can make $a = n - 1 \equiv -1 \mod n$. Since $(-1)^{n-1}$ must be 1, then n must be odd. ∎

More properties of Carmichael numbers

Proposition

Carmichael numbers have no prime factors greater than $\sqrt{n}$.

Proposition

Carmichael numbers have at least 3 prime factors.

Proposition

There are infinitely many Carmichael numbers.

Constructions of Carmichael numbers

Chernick's Construction

Theorem

For an integer k, $(6k+1)(12k+1)(18k+1)$ is a Carmichael number if $6k+1, 12k+1, 18k+1$ are prime.

Proof.

By Korselt's Criterion, we must have $(6k+1)(12k+1)(18k+1)-1$ divisible by $6k, 12k, 18k$. We can rewrite our product to $36k(36k^2+11k+1)$. Since $36k = \text{lcm}(6k, 12k, 18k)$ then our product is divisible by $6k, 12k$, and $18k$. ∎

Other Constructions

There are many more constructions. Here are a few:

1. $(1, 2, 3) \to (6k + 1)(12k + 1)(18k + 1)$
2. $(1, 3, 5) \to (15k + 13)(45k + 37)(75k + 61)$
3. $(1, 2, 5) \to (10k + 7)(20k + 13)(50k + 31)$
4. $(1, 3, 4) \to (12k + 5)(36k + 13)(48k + 17)$
5. $(2, 3, 5) \to (60k + 41)(90k + 61)(150k + 101)$

Other Constructions

1. $(15k+13)(45k+37)(75k+61) \rightarrow$
   $((15k+12)+1)(3(15k+12)+1)(5(15k+12)+1)$
2. $(10k+7)(20k+13)(50k+31) \rightarrow$
   $((10k+6)+1)(2(10k+6)+1)(3(10k+6)+1)$
3. $(12k+5)(36k+13)(48k+17) \rightarrow$
   $((12k+4)+1)(3(12k+4)+1)(4(12k+4)+1)$
4. $(60k+41)(90k+61)(150k+101) \rightarrow$
   $(2(30k+20)+1)(3(30k+20)+1)(5(30k+20)+1)$

Generating Constructions

Definition

Define a Chernick triple (a_1, a_2, a_3) such that a_1, a_2, a_3 share no common factors in total. Then a universal construction is of the form:

$$(a_1(Mk + r) + 1)(a_2(Mk + r) + 1)(a_3(Mk + r) + 1)$$

where $M = \text{lcm}(a_1, a_2, a_3)$ and $0 \leq r < M$.

Remark

Why must $M = \text{lcm}(a_1, a_2, a_3)$?

Generalized solve

Theorem

For a universal construction, $r(a_1a_2 + a_1a_3 + a_2a_3) \equiv -(a_1 + a_2 + a_3) \mod a_1a_2a_3$.

Solving for r is simple now, and we can use extended euclidean algorithm.

Finding Carmichael Numbers

Method 1(bash)

We want to generate pqr that are Carmichael for prime p, q, r. To do this, we will first fix a smallest prime p. From here, we will choose/iterate through a q. To find r, we use the fact that $r-1|pq-1$ by Korselt's Criterion. We will also assume that $p < q < r$.

Lemma

$q < r \leq \frac{pq-1}{2} + 1$

Proof.

Since $(r-1)|(pq-1)$, then $r-1 \leq \frac{pq-1}{2}$. This is because $r-1 \neq pq-1$ since r is prime. ■

Table 1

p	q	$pq-1$	$\frac{pq-1}{2}+1$	r
3	5	14	8	None
3	11	32	17	17
3	17	50	26	None
3	23	68	35	None
5	7	34	18	None
5	13	64	33	17
5	17	84	43	29
5	19	94	48	None
7	11	76	39	None
7	13	90	46	19 and 31
7	17	118	60	None
11	13	142	72	None

Method 2(smarter)

We choose a smallest prime p. Instead of iterating through q, we iterate through h_3. Define $h_3 = \frac{pq-1}{r-1}$ and $h_2 = \frac{pr-1}{q-1}$, for which $d = h_2 h_3 - p^2$. It can be shown that $2 \leq h_3 \leq p-1$.

Remark

One reason for this strange arrangement is that h_3 being integer satisfies $pqr \equiv 1 \mod r-1$ by Korselt's criterion. Another reason for this strange arragement is because this number d depends on p and h_3, for which these properties can be used to solve for h_2.

Proposition

d has the following properties:

1. $d \equiv -p^2 \mod h_3$
2. $d = \frac{(p+h_3)(p+1)}{q-1}$
3. $d \leq p + h_3 - 1$.

Table 2

p	h_3	$-p^2 \mod h_3$	$(p-1)(p+h_3)$	$p+h_3-1$	d	q	r
3	2	$1 \mod 2$	$2*5=10$	4	1	11	17
5	2	$1 \mod 2$	$4*7=28$	6	1	29	73
5	3	$2 \mod 3$	$4*8=32$	7	2	17	29
5	4	$3 \mod 4$	$4*9=36$	8	3	13	17
7	2	$1 \mod 2$	$6*9=54$	8	1	55	
7	2	$1 \mod 2$	$6*9=54$	8	3	19	67
7	3	$2 \mod 3$	$6*10=60$	9	2	31	73
7	3	$2 \mod 3$	$6*10=60$	9	5	13	31
7	4	$3 \mod 4$	$6*11=66$	10	3	23	41
7	5	$1 \mod 5$	$6*12=72$	11	1	73	103
7	5	$1 \mod 5$	$6*12=72$	11	6	13	19
7	6	$5 \mod 6$	$6*13=78$	12			

Table: Iterating using h_3.

Pinch's algorithm

Pinch's algorithm follows a similar method at establishing and finding these Carmichael number by starting with a set of primes and solving for two more primes to find a Carmichael numbers. However, there are a few key differences that set them apart.

Thank You For Listening! Any Questions?