Carmichael Numbers

Structure, Distribution, and Consequences for Primality Testing

Ishaan Mishra

Archbishop Mitty High School, San Jose, California

Motivation: Efficient Primality Testing

The problem

Given an integer n of several hundred digits, decide whether n is prime — in time polynomial in $\log n$.

- Public-key cryptography (RSA) requires large primes generated on demand.
- Trial division tests factors up to $\sqrt{n}$: exponential in $\log n$, infeasible.
- Goal: a test that certifies compositeness *without* producing a factor.

Fermat's Little Theorem

Theorem 1

If p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof outline.

The map $x \mapsto ax$ permutes the nonzero residues $\{1, \ldots, p-1\}$ modulo p (it is injective, since $p \nmid a$ allows cancellation). Multiplying all of them,

$$\prod_{j=1}^{p-1}(aj) \equiv \prod_{j=1}^{p-1} j \implies a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Since p is prime, $(p-1)!$ is invertible mod p; cancel it. □

Cost: a^{p-1} mod p via repeated squaring is $O(\log p)$ multiplications.

The Fermat Primality Test

Contrapositive of Fermat's little theorem:

Test

If $a^{n-1} \not\equiv 1 \pmod{n}$ for some base a, then n is composite.

Definition 2

A base a with $a^{n-1} \not\equiv 1 \pmod{n}$ is a *Fermat witness* for n; a base with $\gcd(a, n) = 1$ and $a^{n-1} \equiv 1 \pmod{n}$ is a *Fermat liar*.

Sample random bases; declare "probably prime" if no witness is found.

Behavior on Small Composites

n	smallest witness a		
15	2	($2^{14} \equiv 4$)	caught immediately
21	2		caught immediately
$341 = 11 \cdot 31$	3	(base 2 is a liar)	caught on 2nd base
561	?		?

- Empirically, witnesses are dense: a few random bases suffice.
- Open question at this stage: is a small witness *guaranteed*, or merely typical?
- The case $n = 561$ answers this.

The Failure Case: $n = 561$

$561 = 3 \cdot 11 \cdot 17$ is composite

Yet $a^{560} \equiv 1 \pmod{561}$ for *every* a with $\gcd(a, 561) = 1$.

No coprime base is a witness. Such composites are **Carmichael numbers**:

$561 = 3 \cdot 11 \cdot 17$	$1105 = 5 \cdot 13 \cdot 17$	$1729 = 7 \cdot 13 \cdot 19$
$2465 = 5 \cdot 17 \cdot 29$	$2821 = 7 \cdot 13 \cdot 31$	$\ldots$

First example found by Šimerka (1885); named for R. Carmichael (1910–12).

Definition and Equivalent Formulation

Definition 3 (Absolute Fermat pseudoprime)

A composite n with $a^{n-1} \equiv 1 \pmod{n}$ for all a coprime to n.

Equivalent, coprimality-free form

$a^n \equiv a \pmod{n}$ for *every* integer a.

Sketch.

($\Leftarrow$) If $\gcd(a, n) = 1$, cancel the unit a from $a^n \equiv a$. ($\Rightarrow$) Reduce mod each prime $p \mid n$: if $p \mid a$ both sides vanish; else $a^{p-1} \equiv 1$ and $(p-1) \mid (n-1)$ give $a^{n-1} \equiv 1$. Squarefree + CRT. □

Contrast: a base-a pseudoprime (e.g. 341, base 2) fails *one* base; a Carmichael number fails all coprime bases at once.

Korselt's Criterion

Theorem 4 (Korselt, 1899)

A composite n is a Carmichael number if and only if

1. *n is squarefree, and*
2. *$(p-1) \mid (n-1)$ for every prime $p \mid n$.*

Replaces infinitely many congruences by a finite check on the factorization.

Example: $n = 561$, $n - 1 = 560 = 2^4 \cdot 5 \cdot 7$

Primes $3, 11, 17 \Rightarrow p - 1 \in \{2, 10, 16\}$, and $2 \mid 560$, $10 \mid 560$, $16 \mid 560$. ✓

Korselt's Criterion: Proof Outline

Necessity — squarefree. If $p^2 \mid n$, pick (CRT) $a \equiv 1 + p \pmod{p^2}$, $a \equiv 1$ elsewhere. Then $\gcd(a, n) = 1$, so mod p^2:

$$1 \equiv a^{n-1} \equiv (1+p)^{n-1} \equiv 1 + (n-1)p \equiv 1 - p \pmod{p^2},$$

forcing $p \equiv 0 \pmod{p^2}$ — contradiction. So n is squarefree.

Necessity — divisibility. Let $p \mid n$; take b a primitive root mod p (order $p-1$), CRT-lift to $a \equiv b\ (p)$, $a \equiv 1\ (n/p)$. Then $a^{n-1} \equiv 1\ (n)$ gives $b^{n-1} \equiv 1 \pmod{p}$, so $(p-1) \mid (n-1)$.

Sufficiency. For $\gcd(a, n) = 1$ and each $p \mid n$: $a^{p-1} \equiv 1$ (Fermat), and $(p-1) \mid (n-1)$ gives $a^{n-1} \equiv 1 \pmod{p}$. Squarefree + CRT $\Rightarrow a^{n-1} \equiv 1 \pmod{n}$.

Structural Properties

Every Carmichael number n satisfies:

1. n **is odd.** $a = -1$: $(-1)^{n-1} \equiv 1$, and $n > 2 \Rightarrow n - 1$ even.
2. n **has** ≥ 3 **distinct prime factors.** If $n = pq$, $p > q$: $\dfrac{n-1}{p-1} = q + \dfrac{q-1}{p-1}$, so $(p-1) \mid (q-1)$ — impossible.
3. $\gcd(n, \varphi(n)) = 1$. If $p_i \mid \varphi(n) = \prod(p_j - 1)$, then $p_i \mid p_j - 1 \mid n - 1$ while $p_i \mid n$: contradiction.

These constraints force n to be squarefree, odd, and prime-poor — hence rare.

Infinitude: Alford–Granville–Pomerance (1994)

Theorem 5

There are infinitely many Carmichael numbers; more precisely,

$$C(x) := \#\{\, n \le x : n \text{ Carmichael} \,\} \;>\; x^{2/7} \quad \text{for all large } x.$$

- Idea (built on Korselt): choose a modulus L so that many primes $p = dk + 1$ have $(p-1) \mid kL$; a product Π of them with $\Pi \equiv 1 \pmod{kL}$ is Carmichael.
- Limitation: pigeonholing over (k, d) loses control of the *size* of Π — it cannot localize Carmichael numbers to a prescribed interval.

Distribution in Intervals and Progressions: Larsen

Larsen (2022) — a Bertrand postulate for Carmichael numbers

For large x there is a Carmichael number in $\left(x,\, x + x/(\log x)^{1/2+\delta}\right)$. Method: Maynard's multidimensional prime sieve + Fourier analysis on $(\mathbb{Z}/kL\mathbb{Z})^\times$ — restoring the size control AGP lacked.

Larsen (2025) — all possible arithmetic progressions

Each progression $r \pmod m$ contains *infinitely many* Carmichael numbers or *none*, decided by an explicit "compatibility" criterion; and $\liminf \varphi(n)/n = 0$ over Carmichael n.

The Fermat Witness Bound

Theorem 6

If a composite n is not Carmichael, then more than half of $\{1, \ldots, n-1\}$ are Fermat witnesses.

Proof outline.

Let $A = \{a \in (\mathbb{Z}/n\mathbb{Z})^\times : a^{n-1} \equiv 1\}$. This is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ (closed under products and inverses). Non-Carmichael $\Rightarrow$ some unit $b \notin A$, so A is *proper*; by Lagrange $[(\mathbb{Z}/n\mathbb{Z})^\times : A] \geq 2$, hence $|A| \leq \varphi(n)/2$. Every non-unit is a witness, so the non-witnesses are exactly A, and $\#\text{witnesses} \geq (n-1) - |A| > \frac{n-1}{2}$. □

Consequence: k random bases miss a non-Carmichael composite with prob. $< 2^{-k}$.

The Carmichael Blind Spot

For a Carmichael number, $A = (\mathbb{Z}/n\mathbb{Z})^\times$: *every* coprime base is a liar.

ordinary composite

Carmichael number

Only witnesses are the non-units; their density is $1 - \varphi(n)/(n-1) \approx \sum_i 1/p_i$, which is negligible for large factors. Since there are infinitely many Carmichael numbers, this blind spot is not eliminable by tabulation.

The Miller–Rabin Test

Write $n - 1 = 2^s d$ with d odd; examine square roots of 1 along $a^d, a^{2d}, \ldots$

Key lemma

Modulo a prime, $x^2 \equiv 1 \Rightarrow x \equiv \pm 1$. A composite with ≥ 2 distinct prime factors has a *nontrivial* square root of 1 (by CRT).

Sketch of the lemma.

$x^2 \equiv 1 \pmod{p} \Rightarrow p \mid (x-1)(x+1) \Rightarrow x \equiv \pm 1$. For $n = n_1 n_2$ coprime, take $x \equiv 1 \ (n_1)$, $x \equiv -1 \ (n_2)$: then $x \not\equiv \pm 1 \pmod{n}$. □

Uniform bound: $\leq \varphi(n)/4$ strong liars for *every* odd composite $n > 9$ — error $\leq (1/4)^k$, **no exceptions**. A Carmichael number ($\omega(n) \geq 3$) has *many* nontrivial roots, so it is caught like any composite.

An Obstruction in Prime Generation

Larsen's criterion: $r \pmod m$ is *incompatible* (Carmichael-free) if, with $g = \gcd(r, m)$, $\lambda = \lambda(g)$, $h = \gcd(\lambda, m)$, any of

$$\gcd(g, 2\varphi(g)) > 1, \quad h \nmid r - 1, \quad (36 \mid m,\ r \equiv 3,\ r/g \equiv 5, 7\ (12)).$$

Proposition 1

Any progression containing a prime $> m$ is Carmichael compatible.

Proof outline.

A prime $> m$ forces $g = \gcd(r, m) = 1$. Then $\gcd(g, 2\varphi(g)) = 1$; $\lambda(1) = 1$ so $h = 1 \mid r - 1$; and $\gcd(r, 12) = 1$ rules out $r \equiv 3\ (12)$. All three conditions fail. □

Consequence: no prime-bearing candidate stream can exclude Carmichael numbers — robustness must come from the *test* (Miller–Rabin), not the distribution.

Summary

- Carmichael numbers are the composites on which the Fermat test degenerates: the liar set A fills the whole unit group.
- Korselt's criterion characterizes them arithmetically (squarefree; $(p-1) \mid (n-1)$), forcing oddness, ≥ 3 prime factors, and $\gcd(n, \varphi(n)) = 1$.
- Distribution: infinite (AGP, $> x^{2/7}$); localized in short intervals and classified across all arithmetic progressions (Larsen, 2022 & 2025).
- Miller–Rabin restores a uniform $(1/4)^k$ bound via nontrivial roots of unity; an obstruction shows this robustness cannot be outsourced to candidate selection.

References

- W. R. Alford, A. Granville, C. Pomerance. *There are infinitely many Carmichael numbers.* Ann. of Math. **140** (1994).
- A. Korselt. *Problème chinois.* L'Interm. des Math. **6** (1899).
- D. Larsen. *Bertrand's postulate for Carmichael numbers.* (2022), arXiv:2111.06963.
- D. Larsen. *Carmichael numbers in all possible arithmetic progressions.* (2025), arXiv:2504.09056.
- G. Miller. *Riemann's hypothesis and tests for primality.* JCSS **13** (1976).
- M. Rabin. *Probabilistic algorithm for testing primality.* J. Number Theory **12** (1980).

Questions?