OURS GOES TO 211: EULER PSEUDOPRIMES TO 47 PRIME BASES FROM CARMICHAEL NUMBERS

ALEJANDRA ALCANTARILLA SANCHEZ[1], JOLIJN COTTAAR[1], TANJA LANGE[1,2], AND BENNE DE WEGER[1]

[1]Eindhoven University of Technology, [2]Academia Sinica Taiwan

We identify Carmichael numbers with the highest density of Euler liars and create a multiplicative algorithm to build a 1230-bit Euler pseudoprime that passes up to base 211, i.e., to 47prime bases.

Definitions

Carmichael Numbers:

Composite n such that $a^{n-1} \equiv 1 \pmod{n}$ for all a coprime to n.

$i(n)$, index of a Carmichael number n:

$$i(n) = \frac{n-1}{\lambda(n)}.$$

$v_2(n)$, 2-adic valuation of an integer n:

Largest integer N such that $2^N \mid n$.

Carmichael Number Classification

Let $n = \prod_{i=1}^{k} p_i$ and let h be the number of factors p_i with $v_2(\lambda(n)) = v_2(p_i - 1)$.

Class	Index	h<k?	# of Euler Liars
A	Even	N.A	$\frac{1}{2}\varphi(n)$
B1	Odd	Yes	$\frac{1}{2^{h+1}}\varphi(n)$
B2	Odd	No	$\frac{1}{2^{k-1}}\varphi(n)$

Why Pseudoprimes?

Public-key cryptography relies on prime numbers.

Primality is often checked using probabilistic tests rather than full proofs.

An adversary can carefully choose composite numbers that can fool such tests.

Solovay-Strassen Test [2]

Euler Pseudoprime to base a:

Odd composite n such that $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}$

epsp(a) :

The set of Euler pseudoprimes that pass all consecutive prime bases until and including a

Why Class A Carmichael Numbers?

Class	Carmichael numbers with smallest factor >150	Found $epsp(a)$, $a \geq 37$	Found $epsp2(a)$, $a \geq 37$
A	7 029 697	128 063	507 767
B1	6 978 344	17	43
B2	271 231	0	0

Multiplication scheme

1. Start from list [1] of Carmichael numbers up to 10^{24}
2. Filter out numbers with small factors
3. Test prime bases and group into epsp(a)
4. Multiply already found Euler Pseudoprimes
5. Keep squarefree Carmichael number products

$\text{epsp}(a_1)$, $\text{epsp}(a_1)$ → $\text{epsp2}(a_2)$; $\text{epsp}(a_2)$ → $\text{epsp3}_{[1,2]}(a)$

Algorithm for Class A Euler Pseudoprimes

Input pairs

Choose n_1 and n_2 in epsp(a) both in Class A, with $v_2(\lambda(n_1)) > v_2(\lambda(n_2))$

Valuation filter $v_2(n_2 - 1) > v_2(\lambda(n_1))$ — No → Reject; Yes

Coprimality filter $\gcd(n_1, n_2) = 1$ — No → Reject; Yes

Build candidate

$n = n_1 n_2, \quad \lambda(n) = \text{lcm}(\lambda(n_1), \lambda(n_2))$

Carmichael filter $\lambda(n) \mid (n-1)$ — No → Reject; Yes

Prime base testing

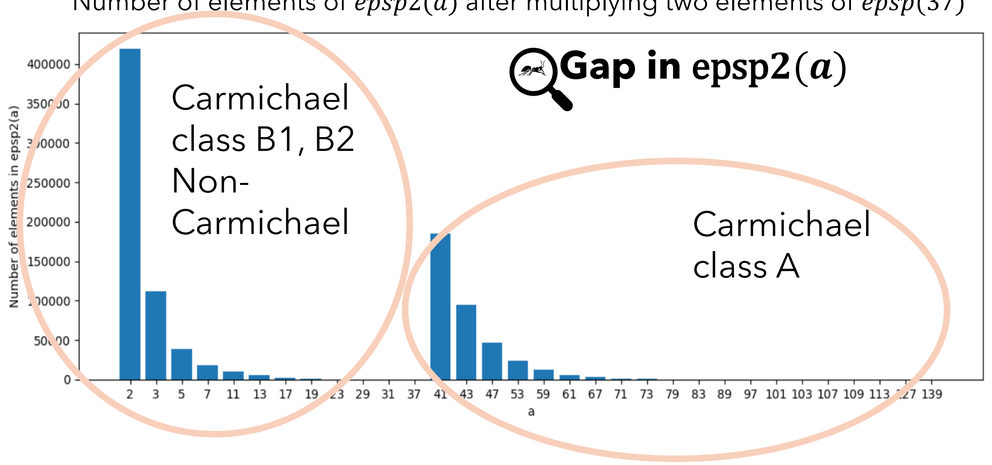
Start from the second prime after a and test consecutive prime bases

Stopping and storing

Stop at first failure and store in corresponding epsp set

Observations

Number of elements of $epsp2(a)$ after multiplying two elements of $epsp(37)$



Mod 120

	% 1 mod 20
Carmichael	88.30
epsp(a)	98.13
epsp($2a$)	99.97

$a > 37$, smallest factor > 150

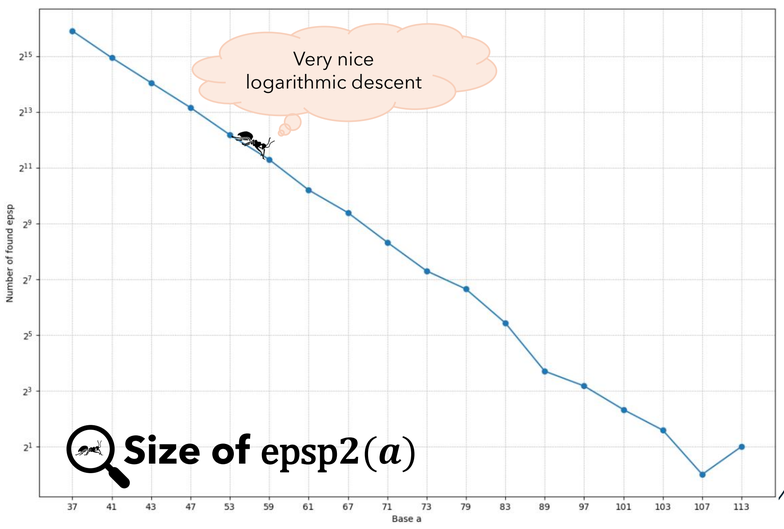
Same base product

	Numbers to check	again *epsp*
epsp2(37) × epsp2(37)	1 895 586 378	0.020 %
epsp2(37) × epsp2(a), $a \geq 41$	4 157 347 387	0.018 %

Totals by construction

epsp(a)	128 080
epsp2(a)	507 810
$\text{epsp3}_{[1,2]}(a)$	4 703 395
$\text{epsp4}_{[2]^2}(a)$	71 300 609
$\text{epsp8}_{[4[2]^2]^2}(a)^*$	49 250 584
$\text{epsp16}_{[8[4[2]^2]^2]^2}(a)^*$	651 128

* : Smaller set of inputs



1230 bits Euler Pseudoprime that survives up to 211

29718025324240318410534115039052540117775597945085067414357453436601387742670453459355591542069934388905907314583289167399384127469613680383642792167067979229668463351656529527558991522533896182769739577451082067252281857005565209955278879251421652977184230025871827972345589832963084011984500975075999311171856228688510024383030748708219201214793184433340476692190457601

REFERENCES

[1] Andrew Shallue and Jonathan Webster. https://blue.butler.edu/~jewebste/new_table. txt, 2025.

[2] Robert M Solovay and Volkert Strassen:. A fast Monte-Carlo test for primality. SIAM J. COMPUT, 6,1977

For more information see:

arXiv:2602.21840