The Density of Pseudoprimes with Two Prime Factors

William F. Galway
Department of Mathematics
University of Illinois at Urbana-Champaign
Urbana, IL 61801
galway@math.uiuc.edu
http://www.math.uiuc.edu/∼galway

Recall "$\mathrm{psp}(n)$" means $2^{n-1} \equiv 1 \bmod n$, n composite and odd. We let p, q, ℓ always denote odd primes. Let

$$P_2(x) = \#\left\{n \le x : n = pq,\ p < q,\ \mathrm{psp}(n)\right\}.$$

Conjecture: Let

$$\delta(m) = \begin{cases} 2 & \text{if } 4 \mid m \\ 1 & \text{otherwise} \end{cases}$$

$$\rho(m) = \prod_{\ell \mid m} \frac{\ell - 1}{\ell - 2}$$

$$T = 2\prod_{\ell} \frac{1 - 2/\ell}{(1 - 1/\ell)^2} \approx 1.320323632\cdots$$

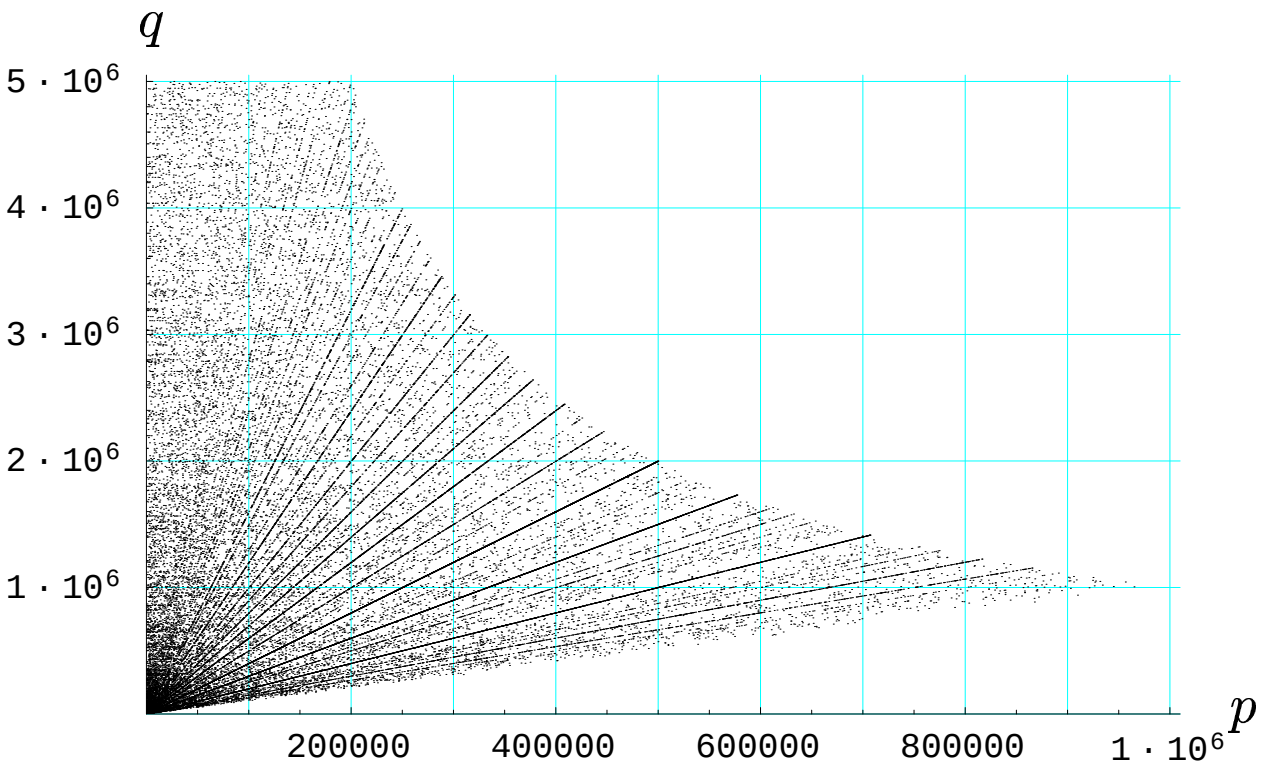
$$C = 4T \sum_{a \ge 1} \sum_{\substack{b > a \\ \gcd(a,b)=1}} \frac{\delta(ab)\,\rho(ab(b-a))}{(ab)^{3/2}} \approx 30.03\cdots$$

Then

$$P_2(x) \sim C\sqrt{x}/\ln^2(x)$$

The Big Picture

Pseudoprimes $pq < 10^{12}$ with $q < 5 \cdot 10^6$.



Overview

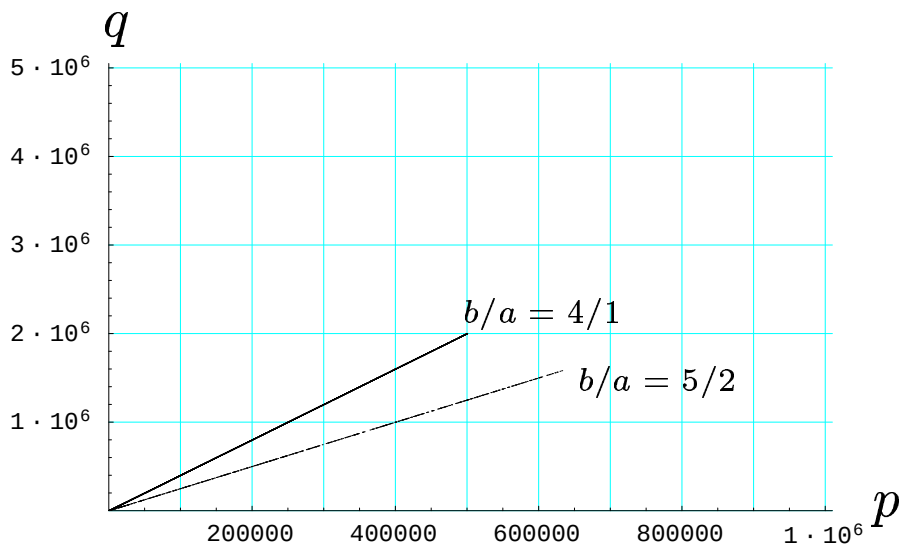
Fix a, b, $a \neq b$, $\gcd(a,b) = 1$ and first estimate

$$\#\left\{p \leq z : \frac{q-1}{p-1} = \frac{b}{a},\ p \ \text{ \& } q \text{ prime}\right\},$$

then estimate

$$\#\left\{p \leq z : \frac{q-1}{p-1} = \frac{b}{a},\ p \ \text{ \& } q \text{ prime},\ \mathrm{psp}(pq)\right\}.$$

Finally, sum over all a, b.



Pairs of Primes on Lines

Conjecture: (Hardy and Littlewood, [HL19], [HL23, Conjecture D])

$$\#\left\{p \le z : \frac{q-1}{p-1} = \frac{b}{a}\right\} \sim \frac{T\rho(ab(b-a))}{a}\frac{z}{\ln^2(z)}$$

where (again) ℓ runs through odd primes,

$$T = 2\prod_{\ell} \frac{1-2/\ell}{(1-1/\ell)^2} \approx 1.320323632\cdots$$

and

$$\rho(m) = \prod_{\ell | m} \frac{\ell - 1}{\ell - 2}$$

Fact: Given odd primes p, q, with $\dfrac{q-1}{p-1} = \dfrac{b}{a}$, then

$$\mathrm{psp}(pq) \iff 2^{(p-1)/a} \equiv 1 \bmod p \;\&\; 2^{(q-1)/b} \equiv 1 \bmod q.$$

The Chebotarëv density theorem implies, for a "random" prime $p \equiv 1 \bmod a$, that

$$\mathrm{Prob}[2^{(p-1)/a} \equiv 1 \bmod p] = \delta(a)/a.$$

Conjecture: (Density of pseudoprimes on lines)

$$\#\left\{p \le z : \frac{q-1}{p-1} = \frac{b}{a},\ \mathrm{psp}(pq)\right\} \sim \frac{T\,\delta(ab)\rho(ab(b-a))}{a^2 b}\frac{z}{\ln^2(z)}$$

Since $pq \le x$ gives $p \le z$ with $z \sim \sqrt{ax/b}$ we expect

$$\#\left\{pq \le x : \frac{q-1}{p-1} = \frac{b}{a},\ \mathrm{psp}(pq)\right\} \sim \frac{4T\,\delta(ab)\rho(ab(b-a))}{(ab)^{3/2}}\frac{\sqrt{x}}{\ln^2(x)}$$

Summing over Lines

Summing over a, b suggests our conjectured formula:

$$P_2(x) \sim C\sqrt{x}/\ln^2(x)$$

with

$$C = 4T \sum_{a \geq 1} \sum_{\substack{b > a \\ \gcd(a,b)=1}} \frac{\delta(ab)\,\rho(ab(b-a))}{(ab)^{3/2}}.$$

Quality of our Conjectures

Pseudoprimes on a line. $b/a = 3/2$, showing

$$N(z) := \#\left\{p \le z : \ \frac{q-1}{p-1} = \frac{b}{a},\ \mathrm{psp}(pq)\right\}$$

versus $z/\ln^2(z)$ and versus

$$\int_0^z \frac{1}{\ln(t)\ln(bt/a)}\,dt.$$

z	$N(z)$	$N(z)\ln^2(z)/z$	$N(z)/\int$
10^4	27	0.2290	0.1774
10^6	1285	0.2453	0.2125
10^8	71697	0.2433	0.2200
∞	...	0.2201	0.2201

Counts of pseudoprimes versus $\sqrt{x}/\ln^2(x)$.

x	$P_2(x)$	$P_2(x)\ln^2(x)/\sqrt{x}$
10^4	11	9.331
10^5	34	14.251
10^6	107	20.423
10^7	311	25.550
10^8	880	29.860
10^9	2455	33.340
10^{10}	6501	34.468
10^{11}	17207	34.908
10^{12}	46080	35.181
10^{13}	123877	35.100
∞	...	$30.03\cdots$

Carmichael Numbers with k Prime Factors

Our conjecture on the density of pseudoprimes with two prime factors is closely related to a conjecture of Granville and Pomerance on the density of Carmichael numbers with k prime factors [GP]. Recall that n is a Carmichael number if n is composite and $a^n \equiv a \bmod n$ for all $a \in \mathbb{N}$.

Conjecture: Let $C_k(x)$ be the counting function for Carmichael numbers with k prime factors, $k \geq 3$. Then

$$C_k(x) \sim \tau_k \, x^{1/k} / \ln^k(x)$$

for some $\tau_k > 0$.

References

[GP] Andrew Granville and Carl Pomerance, *Two contradictory conjectures concerning Carmichael numbers*, (to appear).

[HL19] G. H. Hardy and J. E. Littlewood, *Note on messrs Shah and Wilson's paper entitled: 'on an empirical formula connected with Goldbach's theorem'*, Proceedings of the Cambridge Philosophical Society **19** (1919), 245–254.

[HL23] G. H. Hardy and J. E. Littlewood, *Some problems of 'partitio numerorum'; III: on the expression of a number as a sum of primes*, Acta Mathematica **44** (1923), 1–70.

[Pin] R. G. E. Pinch, *Lists of pseudoprimes below* 10^{13}, `ftp://ftp.dpmms.cam.ac.uk/pub/rgep/PSP/`.

[Pin00] R. G. E. Pinch, *The pseudoprimes up to* 10^{13}, Algorithmic Number Theory (ANTS-IV) (Wieb Bosma, ed.), Lecture Notes in Computer Science, vol. 1838, Springer, Berlin, July 2000, pp. 459–473.