Order and chaos

Carl Pomerance, Dartmouth College
Hanover, New Hampshire, USA

Arithmetic Statistics, Introductory Workshop
February 1, 2011

Perfect shuffles

Suppose you take a deck of 52 cards, cut it in half, and perfectly shuffle it (with the bottom card staying on the bottom).

If this is done 8 times, the deck returns to the order it was in before the first shuffle.

But, if you include the 2 jokers, so there are 54 cards, then it takes 52 shuffles, while a deck of 50 cards takes 21 shuffles.

What's going on?

Persi Diaconis

Let Shuf($2k$) denote the number of perfect shuffles that will return a deck of $2k$ cards to the order it was in before shuffling.

So, Shuf(50) = 21, Shuf(52) = 8, Shuf(54) = 52.

When a small change in input can produce a large change in output, we are looking at a *chaotic* function. It appears that Shuf is chaotic.

Here's another example. Consider the length of the repeating period for the decimal for $1/n$. Let this be denoted Peri(n), so for example, Peri(3) = 1, Peri(7) = 6. Here are some values for odd numbers starting above 100:

Peri(101) = 4

Peri(103) = 34

Peri(105) = 6

Peri(107) = 53

Peri(109) = 108

Peri(111) = 3

Peri(113) = 112

For a positive integer n coprime to an integer a, let $l_a(n)$ denote the multiplicative order of a in $(\mathbb{Z}/n\mathbb{Z})^\times$.

As I'm sure all here know, when n is coprime to 10, we have $\mathrm{Peri}(n) = l_{10}(n)$.

There is a connection here too with $\mathrm{Shuf}(2k)$.

Note that

$$l_2(49) = 21, \quad l_2(51) = 8, \quad l_2(53) = 52.$$

In fact, it is not hard to prove that $\mathrm{Shuf}(2k) = l_2(2k-1)$.

(Number the cards 0 to $2k-1$, with 0 the top card. Then a perfect shuffle takes a card in position i and sends it to $2i \bmod (2k-1)$.)

We see that the order function $l_a(n)$ is chaotic, thus explaining the title of this lecture.

Trying to understand the order function has applications in cryptography, for example in computing the periods of certain pseudo-random number generators. And of course the RSA cryptosystem relies for its security on the difficulty in computing the order function.

Further, as a basic and ubiquitous number-theoretic function it seems interesting to study $l_a(n)$ from a statistical viewpoint.

What are extreme values for $l_a(n)$?

What is it normally?

What is it on average?

In fact analytic number theory is quite well acquainted with chaotic functions. Take the divisor function $d(n)$, which counts the number of positive divisors of n. For example,

$$d(2309) = 2, \quad d(2310) = 32, \quad d(2311) = 2.$$

This behavior is tamed by looking at $d(n)$ on average. In fact

$$\frac{1}{x} \sum_{n \le x} d(n) = \log x + c + o(1), \quad \text{as } x \to \infty.$$

It is easy to investigate the sum, since we can replace $d(n)$ with

$$\sum_{d|n} 1,$$

and then interchange the order of summation. (To get the constant and a reasonable error estimate, one uses the symmetry $d \leftrightarrow n/d$.)

Another example of how an elementary number-theoretic function may be studied statistically: $\omega(n)$, the number of divisors of n that are prime. It is more gentle than $d(n)$, for example

$$\omega(2309) = 1, \quad \omega(2310) = 5, \quad \omega(2311) = 1.$$

It is easy to show that

$$\frac{1}{x} \sum_{n \le x} \omega(n) = \log\log x + c + o(1).$$

Thus, the average order of $\omega(n)$ is $\log\log n$. This is also the "normal order": for each $\epsilon > 0$, the set of integers n with

$$(1 - \epsilon) \log\log n < \omega(n) < (1 + \epsilon) \log\log n$$

has asymptotic density 1 (Hardy & Ramanujan, Turán).



Godfrey Harold Hardy Pál Turán

Srinivasa Ramanujan

Talk about Arithmetic Statistics, we even have the bell curve showing up. After Erdős & Kac, we know that for each real number u, the asymptotic density of the set of integers n with

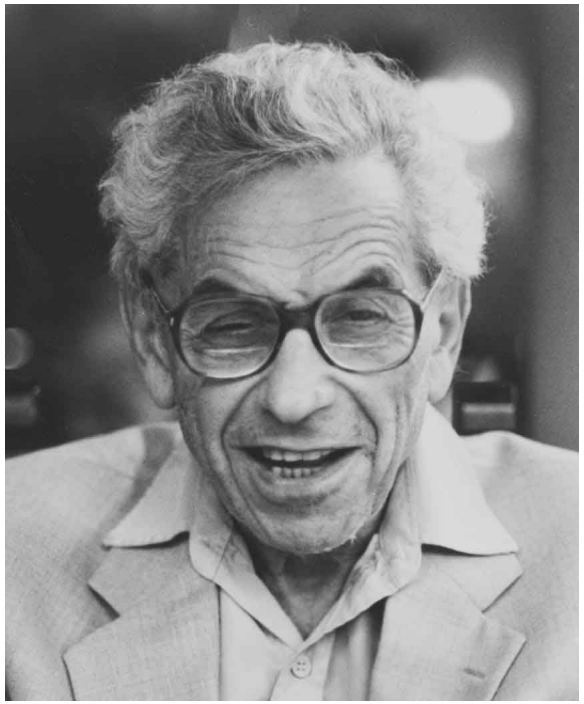
$$\omega(n) \leq \log\log n + u\sqrt{\log\log n}$$

is

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{u} e^{-t^2/2}\, dt,$$

the Gaussian normal distribution.

(Erdős & Kac did *not* remark: 'Einstein says that God does not play dice with the universe. Maybe so, but something is going on with the primes.')



Paul Erdős

Mark Kac

The work on the normal order of $\omega(n)$ and the average order of $d(n)$ shows that $d(n)$ is for most values of n about $(\log n)^{\log 2}$ but on average it is about $\log n$. That is, what is normal is far from what is average.

There are other statistical surprises in elementary number theory. For example, on average, a number n has $\log 2$ divisors between $\frac{1}{2}\sqrt{n}$ and $\sqrt{n}$, but almost all numbers n have no divisors in this interval.

Here is another: We know that the number of integers n with $\varphi(n) \le x$ is $cx + o(x)$ as $x \to \infty$, where $c = \zeta(2)\zeta(3)/\zeta(6)$. It is also known that under assumption of the Elliott–Halberstam conjecture, there is *no* power-saving error term in this result.

How does one begin to study $l_a(n)$?

Since $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$, we have $l_a(n) \mid \varphi(n)$.

However, we can do better: An elementary result that goes back to Gauss and Carmichael is that $l_a(n) \mid \lambda(n)$.

Here $\lambda(n) = \max_{(a,n)=1} l_a(n)$, the order of the largest cyclic subgroup in $(\mathbb{Z}/n\mathbb{Z})^\times$. We have

$$\lambda([m,n]) = [\lambda(m), \lambda(n)], \qquad \lambda(p^j) = \varphi(p^j) = p^{j-1}(p-1)$$

for odd primes p and $p^j = 2$ or 4, and $\lambda(2^j) = 2^{j-2}$ for $j \geq 3$.

So the largest $l_a(n)$ can be is $\lambda(n)$. How often does this occur?

If $l_a(n) = \lambda(n)$, we say that a *is a primitive root for* n, thus generalizing the usual terminology when $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic.

Let $R(n)$ denote the number of primitive roots for n in $(\mathbb{Z}/n\mathbb{Z})^\times$. When $n = p$ is prime we have $R(p) = \varphi(p-1)$, and it is not hard to prove (Stephens) that

$$\sum_{p \le x} \frac{R(p)}{p} = \sum_{p \le x} \frac{\varphi(p-1)}{p} \sim A\pi(x), \quad x \to \infty,$$

where

$$A = \prod_p \left(1 - \frac{1}{p(p-1)}\right) = 0.3739558136\ldots$$

is known as Artin's constant.

Here is a proof. Changing the summand $\varphi(p-1)/p$ to $\varphi(p-1)/(p-1)$ changes the sum by less than the sum of $1/p$ for $p \le x$, which is negligible compared with $\pi(x)$. Further, we can write $\varphi(p-1)/(p-1)$ as the sum of $\mu(d)/d$ over $d \mid p-1$. Thus,

$$\sum_{p\le x} \frac{\varphi(p-1)}{p-1} = \sum_{p\le x} \sum_{d\mid p-1} \frac{\mu(d)}{d} = \sum_{d\le x} \frac{\mu(d)}{d} \pi(x; d, 1).$$

We would like to replace $\pi(x; d, 1)$ with $\pi(x)/\varphi(d)$, but this is not known to be a good approximation for all d in this vast range, not even on average. We do know it uniformly (and effectively) in the range $d \le (\log x)^{3/2}$ and this is sufficient since we can replace the remaining terms with the upper bound x/d^2 whose sum is $O(x/(\log x)^{3/2})$.

Thus, taking into account the various errors introduced, we have

$$\sum_{p\leq x}\frac{\varphi(p-1)}{p}=\pi(x)\sum_{d=1}^{\infty}\frac{\mu(d)}{d\varphi(d)}+O\left(\frac{x}{(\log x)^{3/2}}\right),$$

and it remains to note that

$$\sum_{d=1}^{\infty}\frac{\mu(d)}{d\varphi(d)}=\prod_{p}\left(1-\frac{1}{p(p-1)}\right)=A.$$

Let $P_a(x)$ denote the number of primes $p \leq x$ for which a is a primitive root for p. It is perhaps natural to conjecture that the particular residue a is just as likely to be a primitive root for p as is a random residue, that is,

$$P_a(x) \sim A\pi(x), \quad x \to \infty.$$

However, this is clearly wrong! For example, take $a = 0$, $a = 1$, $a = 4$, more generally, $a = \square$, or $a = -1$. Then $P_a(x) \leq 2$ for all x. So the "correct" conjecture is that for $a \neq -1, \square$, there is a positive number A_a with $P_a(x) \sim A_a\pi(x)$. (The need to have the constant vary with a comes from algebraic number theory, the case when a is a cube, and similar.)

A weak form of this was first conjectured by Gauss, but it is now known as Artin's conjecture. It was proved by Hooley under the assumption of the Riemann hypothesis for algebraic number fields of the form $\mathbb{Q}(a^{1/n}, \zeta_n)$.

Corollary. If this GRH holds, then for infinitely many deck sizes $2k$, the number of perfect shuffles to return it to its order before shuffling is $2k - 2$.

Corollary. If this GRH holds, then for infinitely many primes p, the length of the period for the decimal of $1/p$ is $p - 1$.

Carl Friedrich Gauss

Emil Artin

It should be easy to formulate a version of Artin's conjecture for composites, right? Namely, prove that

$$\sum_{n \le x} \frac{R(n)}{n} \sim Bx, \quad x \to \infty$$

for some constant $B > 0$, and then posit that for each number a outside of some exceptional set there is a positive number B_a with $N_a(x) \sim B_a x$, where $N_a(x)$ is the number of $n \le x$ for which a is a primitive root (that is, $l_a(n) = \lambda(n)$).

OK, to get started, we should work out a formula for $R(n)$. Often it is $\varphi(\varphi(n))$, but not always. For each prime $q \mid \lambda(n)$, let e_q be the exponent on q in the factorization of $\lambda(n)$, and let $\Delta_q(n)$ be the q-rank of

$$\left((\mathbb{Z}/n\mathbb{Z})^\times\right)^{\lambda(n)/q}.$$

So, $\Delta_q(n)$ is the number of factors $C_{q^{e_q}}$ in $(\mathbb{Z}/n\mathbb{Z})^\times$. With the numbers $\Delta_q(n)$ we can write down a formula for $R(n)$:

Li, Martin: $R(n) = \varphi(n) \prod_{q|\lambda(n)} \left(1 - q^{-\Delta_q(n)}\right)$.

But what about $\mathcal{R}(x) := \sum_{n \le x} R(n)/n$? Recall our plan is to show that $\mathcal{R}(x) \sim Bx$. But ...

Li: The function $\mathcal{R}(x)$ oscillates. In fact,

$$\limsup_{x\to\infty} \mathcal{R}(x)/x > 0, \quad \liminf_{x\to\infty} \mathcal{R}(x)/x = 0.$$

What's going on?

Shuguang Li

Greg Martin

Consider a game where you have a chance to win a quarter:

I give you n quarters, you flip them all, and return to me all that land tails.

You repeat this over and over, but if you get down to a single quarter, you get to keep it. (So, for example, if you have 2 quarters at one point, you flip them, and they both come up tails, you lose.)

What is the probability of winning as $n \to \infty$? If you work it out numerically it appears to converge to some positive number, but in fact, it does not converge, it oscillates slightly. (If n tends to infinity through a subsequence where $\{\log n / \log 2\}$ converges to θ, then the probability converges to some $f(\theta)$.)

So, what does this have to do with primitive roots? Well, in the formula for $R(n)$ there's a factor $1 - 2^{-\Delta_2(n)}$, so it is of interest to know how frequently $\Delta_2(n) = 1$, how frequently it is 2, etc. Analogous to quarters are the prime powers q^b in the prime factorization of n. The quarters which turn tails on the first round are those q^b with $q \equiv 3 \pmod 4$ (and when $q = 2$: if $\lambda(2^b) = 2$). The ones that turn tails on the next round are those with $q \equiv 5 \pmod 8$, etc. The number of quarters remaining on the final round corresponds to $\Delta_2(n)$. Since n has usually about $\log\log n$ prime divisors, we should get one situation for $\Delta_2(n)$ if $\log\log n$ is close to a power of 2, and another if it is close to a number $2^{k+1/2}$.

This kind of game is repeated for each small prime, not just 2. If $\log\log n$ is well approximated by powers of each small prime, we get one kind of behavior, and if it is far from being well approximated by small prime powers, we get another kind of behavior.

Thus, the oscillation. But it is very gentle. We know (Li) that $\mathcal{R}(x) \gg x/\log\log\log x$.

Using these kinds of ideas, Li showed that

$$\liminf_{x\to\infty} N_a(x)/x = 0$$

for any fixed number a. ($N_a(x)$ is the number of $n \leq x$ coprime to a with $l_a(n) = \lambda(n)$.)

And assuming GRH, Li, P showed that for a outside of an exceptional set,

$$\limsup_{a\to\infty} N_a(x)/x > 0.$$

(For a exceptional, $N_a(x) = o(x)$.) In a new result, Li, P showed unconditionally that for $y \geq \exp((2+\epsilon)\sqrt{\log x \log\log x})$, we have

$$\sum_{1\leq a\leq y} N_a(x) \sim y\mathcal{R}(x).$$

Long ago, Stephens had a similar unconditional result for $P_a(x)$.

Now we turn to the order function $l_a(n)$ normally and on average.

For λ, we do have results about it's normal and average order, and they are a far cry from a possible first guess, the normal and average orders of φ.

Erdős, P, Schmutz: *On a set of asymptotic density 1,*

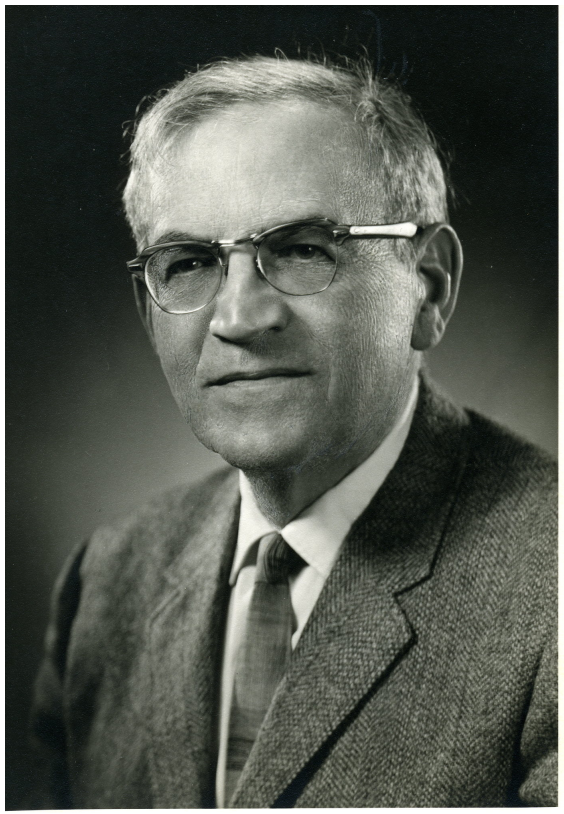
$$\lambda(n) = n/(\log n)^{\log\log\log n + C + o(1)}$$

for a certain explicit positive constant C*.*

This should be compared with

Schoenberg: *For each real number* $u \in [0,1]$ *let* $\delta(u)$ *denote the asymptotic density of the integers* n *with* $\varphi(n) \leq un$*. Then* $\delta(u)$ *exists and the function* δ *is continuous and strictly increasing on* $[0,1]$*.*

Eric Schmutz



Isaac Jacob Schoenberg

Erdős, P, Schmutz: *As* $x \to \infty$,

$$\frac{1}{x}\sum_{n\le x}\lambda(n) = \frac{x}{\log x}\exp\left(\frac{(D+o(1))\log\log x}{\log\log\log x}\right)$$

for a certain explicit positive constant D.

This should be compared with the classical result that

$$\frac{1}{x}\sum_{n\le x}\varphi(n) \sim cx \text{ as } x \to \infty,$$

where $c = 1/(2\zeta(2)) = 3/\pi^2$.

Further, assuming GRH, most n coprime to a have $\lambda(n)/l_a(n)$ small. (Results of Li, Kurlberg, and Li & P.)

Thus, one has

$$l_a(n) = n/(\log n)^{\log\log\log n + C + o(1)}$$

for almost all n coprime to a.

Clearly the average order of $\lambda(n)$, which is of greater magnitude than $n/\log n$, is much larger than the normal order, so the average is determined by a thin set of numbers with abnormally large values of λ. Thus, it is unclear what is happening with the average order of $l_a(n)$.

After some numerical experiments, V. I. Arnold recently concluded that on average $l_a(n)$ is $C_a n/\log n$, and he gave a heuristic argument for this based on the physical principle of turbulence. This is in the paper

Number-theoretical turbulence in Fermat–Euler arithmetics and large Young diagrams geometry statistics, *Journal of Fluid Mechanics* **7** (2005), S4–S50.

It seems to have been discussed in one of the *Chern Lectures* he gave at UC Berkeley in 2007.

Vladimir I. Arnold

Arnold writes in the abstract:

"Many stochastic phenomena in deterministic mathematics had been discovered recently by the experimental way, imitating Kolmogorov's semi-empirical methods of discovery of the turbulence laws. From the deductive mathematics point of view most of these results are not theorems, being only descriptions of several millions of particular observations. However, I hope that they are even more important than the formal deductions from the formal axioms, providing new points of view on difficult problems where no other approaches are that efficient."

And he asserts that his expression $C_a n/\log n$ for the average order of $l_a(n)$ (in the case $a = 2$) is in fact supported by *billions* of experiments.

I think we should be a bit suspicious!

First, iterated logarithms grow so slowly that they are difficult to detect numerically.

Second, Arnold did not seem to investigate any of the literature dealing with $l_a(n)$. In fact, there are interesting papers on the subject going back to Romanoff (who proved that the sum of $1/(nl_a(n))$ for n coprime to a is convergent), with later papers by Erdős, P, Pappalardi, Li, Kurlberg, Murty, Rosen, Silverman, Saidak, Moree, Luca, Shparlinski, and others.

But...

It's good to have outsiders investigate a field, and if they were expected to first read the literature thoroughly, it might dampen the fresh insight they might bring.

And, his conjecture that the average order of $l_2(n)$ grows like $n/\log n$ is supported on one side by Hooley's GRH-conditional proof of Artin's conjecture. Thus, assuming the GRH, a positive proportion of primes p have $l_2(p) = p - 1$, so that just the contribution of primes to the sum of $l_2(n)$ gives an average order that is $\gg n/\log n$. And perhaps composites do not contribute too much.

However...

Shparlinski (2007): *Let* $|a| > 1$. *Assuming the GRH, there is some* $C_a > 0$ *with*

$$\frac{1}{x} \sum_{\substack{n \le x \\ (a,n)=1}} l_a(n) \ge \frac{x}{\log x} \exp\left(C_a (\log\log\log x)^{3/2}\right).$$

(On some dynamical systems in finite fields and residue rings, *Discrete and continuous dynamical systems, Series A* **17** (2007), 901–917.)

And he suggests that with more work, the exponent "3/2" might possibly be replaced with "2".

Igor Shparlinski

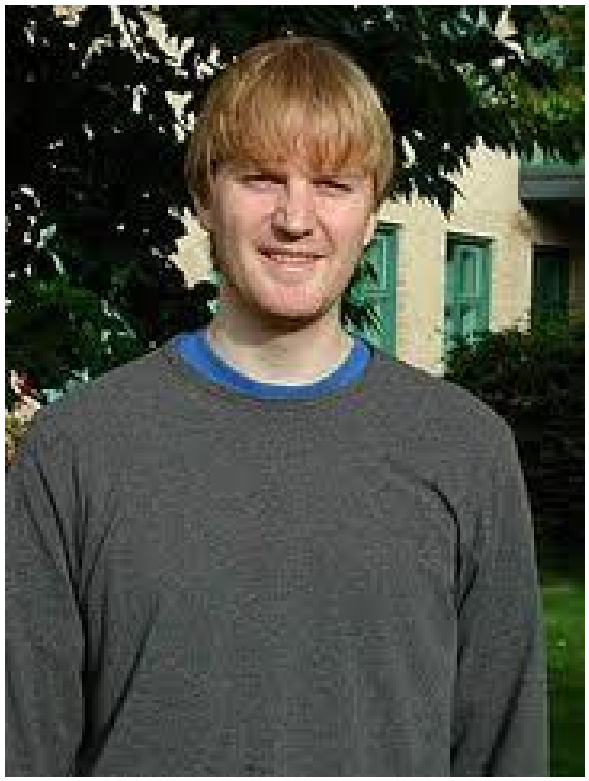
Kurlberg and P: *Let* $|a| > 1$. *Assuming the GRH,*

$$\frac{1}{x} \sum_{\substack{n \le x \\ (a,n)=1}} l_a(n) = \frac{x}{\log x} \exp\left(\frac{(D + o(1)) \log\log x}{\log\log\log x} \right).$$

Here "D" is the same constant that appears in the average order of $\lambda(n)$, namely

$$D = e^{-\gamma} \prod_p \left(1 - \frac{1}{(p-1)^2(p+1)} \right) = 0.3453720641\ldots .$$

In particular, the upper bound in the theorem holds unconditionally.



Pär Kurlberg

The proof is a bit intense, borrowing heavily from the structure of the proof in Erdős, P, & Schmutz of the corresponding result for $\lambda(n)$.

However, the following lemma is also used:

Kurlberg & P (2005): *For* $1 \le y \le \log x / \log\log x$

$$\#\{p \le x : l_a(p) < p/y\} = O\left(\frac{\pi(x)}{y}\right).$$

This result follows essentially from the the Hooley GRH conditional proof of Artin's primitive-root conjecture. (Pappalardi (1996) had this result in a wider range for y, but it has been retracted. Kurlberg (2003) had this result in the range $y \le (\log x)^{1-\varepsilon}$.)

We also have begun to consider the somewhat easier problem that perhaps has not been considered before: What can one say about $l_a(p)$ on average over primes p?

For example, take $a = 2$; then we have the following result:

Assume the GRH. The average order of $l_2(p)$ *is* $\frac{159}{160}cp$*, where*

$$c = \prod_p \left(1 - \frac{p}{p^3 - 1}\right).$$

Note that $\frac{159}{160}c = 0.57236022\ldots$, so that on average, $l_2(p) > \frac{4}{7}p$.

Luca (2002) has shown that the average order of an element in the group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cp on average. (Two levels of averaging.)

That is, he shows that

$$\sum_{p \le x} \sum_{a=1}^{p-1} l_a(p) \sim \frac{1}{3} c x^2 \pi(x), \quad x \to \infty.$$

Hu (2010) has worked out a similar result for orders in finite fields of a given fixed degree over their prime fields.

Florian Luca

Yilan Hu

I conclude with a proof of Luca's theorem.

Let $f(p) = \sum_{a=1}^{p-1} l_a(p)$, so that

$$f(p) = \sum_{d|p-1} d\varphi(d) = \sum_{d|p-1} \varphi(d^2) = \sum_{d|p-1} \varphi\left(\left(\frac{p-1}{d}\right)^2\right).$$

Thus,

$$S := \sum_{p\le x} f(p) = \sum_{d\le x} \sum_{\substack{p\le x \\ d|p-1}} \varphi\left(\left(\frac{p-1}{d}\right)^2\right).$$

The contribution to S from values of $d > x^{1/5}$ is at most

$$\sum_{d>x^{1/5}} \frac{x}{d}\cdot\frac{x^2}{d^2} = O(x^{2.6}).$$

The remaining part of S is

$$\sum_{d\le x^{1/5}} \sum_{\substack{p\le x\\ d\mid p-1}} \left(\frac{p-1}{d}\right)^2 \sum_{e\mid (p-1)/d} \frac{\mu(e)}{e}.$$

Using that no integer below x has more than x^ϵ divisors, the contribution here when $e > x^{1/5}$ is at most

$$\sum_{d\le x^{1/5}} \frac{x}{d}\cdot\frac{x^2}{d^2}\cdot\frac{x^\epsilon}{x^{1/5}} = O(x^{2.8+\epsilon}).$$

Thus, we are left to estimate

$$\sum_{d,e\le x^{1/5}} \sum_{\substack{p\le x\\ de\mid p-1}} \frac{(p-1)^2\mu(e)}{d^2 e}.$$

The sum on p may be estimated via the Bombieri–Vinogradov theorem, and so we get,

for any fixed number A,

$$S = \mathrm{li}(x^3) \sum_{d,e \le x^{1/5}} \frac{\mu(e)}{d^2 e \varphi(de)} + O(x^3/(\log x)^A).$$

The remaining sum may be extended over all d, e, and note that

$$\sum_{d,e} \frac{\mu(e)}{d^2 e \varphi(de)} = \sum_{d,e} \frac{\mu(e) e}{d^2 e^2 \varphi(de)} = \sum_n \frac{1}{n^2 \varphi(n)} \sum_{e|n} \mu(e) e.$$

The inner sum is $(-1)^{\omega(n)} \mathrm{rad}(n) \varphi(n)/n$, so the sum becomes

$$\sum_n \frac{(-1)^{\omega(n)} \mathrm{rad}(n)}{n^3} = \prod_p \left(1 - \frac{p}{p^3 - 1}\right) = c.$$

We conclude that $S = c\,\mathrm{li}(x^3) + O(x^3/(\log x)^A)$, proving the theorem.

Further reading:

V. I. Arnold, *Number-theoretical turbulence in Fermat–Euler arithmetics and large Young diagrams geometry statistics*, J. Fluid Mechanics **7** (2005), S4–S50.

P. Kurlberg and C. Pomerance, in progress.

P. Erdős, C. Pomerance, and E. Schmutz, *Carmichael's lambda function*, Acta Arith. **58** (1991), 363–385.

C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.

S. Li and C. Pomerance, *On the Artin–Carmichael primitive root problem on average*, Mathematika **55** (2009), 167–176.