A Problem of Arnold on the average multiplicative order

Carl Pomerance, Dartmouth College
Hanover, New Hampshire, USA

Maine/Québec Number Theory Conferece, 2011

This talk concerns the function $\ell_a(n)$ which gives the order of an integer a in the mulitiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$, the group of units modulo n. It is assumed that a is in the group of course, that is, $\gcd(a, n) = 1$.

We know that $\ell_a(n) \mid \varphi(n)$, since $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$.

Can we say more in general?

In an abelian group, if elements a, b have coprime orders, then the order of ab is the product of the two orders. One deduces from this that each element's order in the group divides the maximal order. This maximal order is known as the *universal exponent*.

Let $\lambda(n)$ denote the universal exponent for $(\mathbb{Z}/n\mathbb{Z})^*$. Using the Chinese Remainder Theorem plus the theorem that $(\mathbb{Z}/p^k\mathbb{Z})^*$ is cyclic for odd primes p and for $p^k = 2, 4$, and has a cyclic subgroup of index 2 when $p = 2$ and $k \geq 3$, we can compute $\lambda(n)$ from the prime factorization of n.

We have $\lambda(p^k) = \varphi(p^k)$ for p an odd prime and for $p^k = 2$ or 4, and $\lambda(2^k) = \frac{1}{2}\varphi(2^k) = 2^{k-2}$ for $k \geq 3$. In addition, for any integers m, n we have

$$\mathrm{lcm}[\lambda(m), \lambda(n)] = \lambda(\mathrm{lcm}[m, n]).$$

For example,

$$\lambda(1001) = \lambda(\mathrm{lcm}[7, 11, 13]) = \mathrm{lcm}[6, 10, 12] = 60,$$

while

$$\varphi(1001) = \varphi(7)\varphi(11)\varphi(13) = 6 \cdot 10 \cdot 12 = 720.$$

We always have for every integer a coprime to n,

$$\ell_a(n) \mid \lambda(n).$$

And, in general, we expect for most numbers n, that $\lambda(n)$ is a relatively small divisor of $\varphi(n)$.

The function $\ell_a(n)$ can be viewed as a function of n, where we take a as a fixed integer, and the function is defined when $\gcd(a, n) = 1$. As such, it is a fairly erratic function. For example,

$$\ell_2(51) = 8, \quad \ell_2(53) = 52,$$

which is what is behind the fact that 8 “perfect shuffles” of a 52-card deck restores the starting order of the cards, while if the two jokers are included, it takes 52 perfect shuffles.

When faced with erratic behavior, it becomes interesting to look at the situation statistically. This is where V. I. Arnold enters the picture.

When faced with erratic behavior, it becomes interesting to look at the situation statistically. This is where V. I. Arnold enters the picture.

Vladimir I. Arnold

The question of the average order of $\ell_a(n)$ for a fixed was recently discussed by V. I. Arnold.

After some numerical experiments, he concluded that

$$\frac{1}{x}\sum_{n\le x}\ell_a(n)\sim C_a\frac{x}{\log x}.$$

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.

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 says that his conjecture is supported by *billions* of experiments.

I think we should be a bit suspicious!

First, even billions of experiments may not be enough to tease out extra factors that may grow more slowly than $\log x$.

Second, Arnold did not seem to investigate any of the literature dealing with $\ell_a(n)$. In fact, there are interesting papers on the subject going back to Romanoff (who proved that the sum of $1/(n\ell_a(n))$ 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.

In addition he seemed to be unaware of work done on $\lambda(n)$.

There is some famous work concerning $\ell_a(p)$ where p is a prime not dividing the integer a. Recall that $\ell_a(p) \mid \lambda(p) = p - 1$. And, there are choices for a where $\ell_a(p) = p - 1$.

For example, with $a = 2$ and $p = 53$.

Another example is with $a = 10$ and $p = 109$. So the length of the repeating period for the decimal expansion of $1/109$ is 108.

Over two centuries ago, Gauss asked if this deal with the decimal for $1/p$ occurred for infinitely many primes p. I.e., do we have $\ell_{10}(p) = p - 1$ for infinitely many primes p?

In the mid twentieth century, Artin generalized Gauss's conjecture as follows.

Suppose that a is an integer which is not a square and not -1. The Artin conjecture: *There is a positive constant $A(a)$ such that asymptotically the proportion of primes p with $\ell_a(p) = p - 1$ among all primes tends to $A(a)$.*

This is still not proven, nor even the weaker assertion that there are infinitely many primes p with $\ell_a(p) = p - 1$. (This is the Gauss conjecture when $a = 10$.)

However, the full Artin conjecture is known *conditionally* under the assumption of the Generalized Riemann Hypothesis, a theorem of Hooley.

Carl Friedrich Gauss

Emil Artin

One could ask about analogies for composite numbers.

A natural generalization of the Gauss–Artin problem:
For a fixed integer a outside of some sparse exceptional set, do we have $\ell_a(n) = \lambda(n)$ for a positive proportion $B(a)$ of integers n relatively prime to a?

In recent work with Li, we showed that under the assumption of the Generalized Riemann Hypothesis, the density of such integers n does *not* exist: the limsup of the density is indeed a positive number $B(a)$, but the liminf is 0.

Shuguang Li

Let us return to the statistical problem of Arnold.

He asked about the average value of $\ell_a(n)$ as n varies. Instead, we could study the average value of $\ell_a(p)$ as p varies. One too could consider the average as a function of a or over both variables. For example, Luca worked out the asymptotic behavior of

$$\sum_{p\le x}\sum_{a=1}^{p-1}\ell_a(p)$$

and Hu and I did the analogous thing for more general finite fields.

Florian Luca

Yilan Hu

For $\ell_a(n)$ we could ask first the easier question: What is the average value of $\lambda(n)$? (Recall that we always have $\ell_a(n) \mid \lambda(n)$ and often they are equal.)

What this question means is: How does

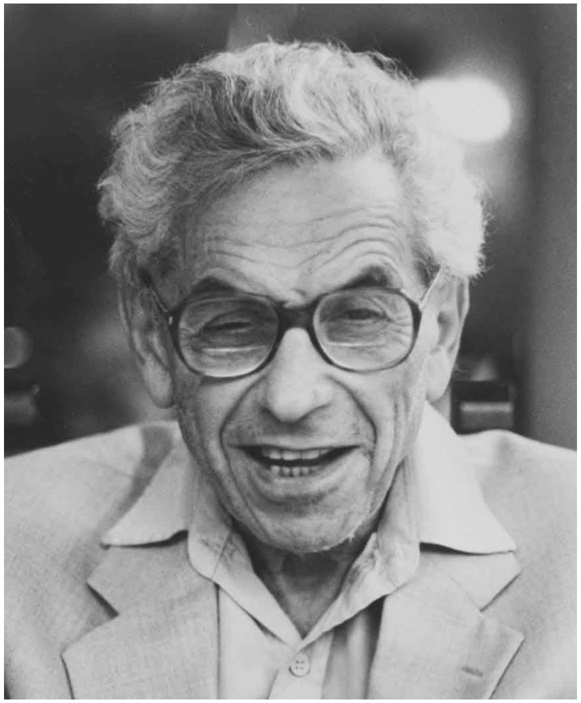
$$\frac{1}{x}\sum_{n\le x}\lambda(n)$$

behave as $x \to \infty$?

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.



Paul Erdős

Eric Schmutz

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

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

(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

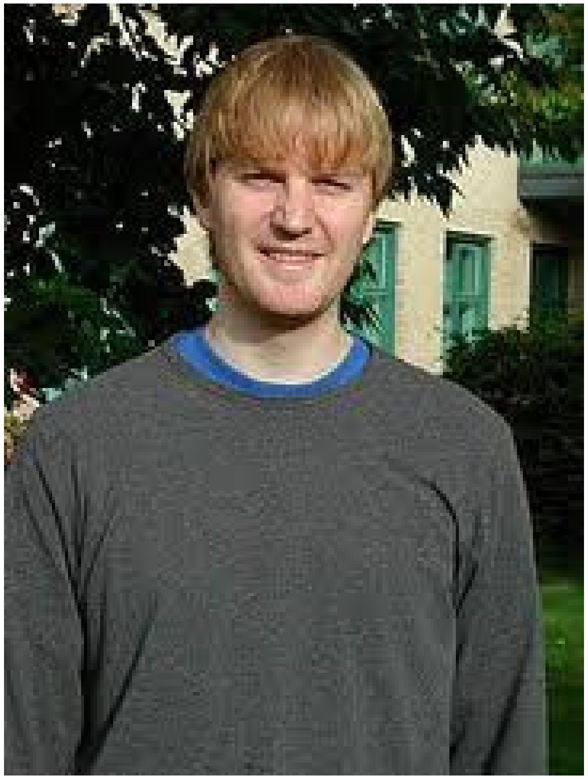
Kurlberg and P: *Let $|a| > 1$. Assuming the Generalized Riemann Hypothesis,*

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

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

$$D = e^{-\gamma} \prod_p \left(1 - \frac{1}{(p-1)^2 (p+1)} \right) = 0.345372\ldots.$$

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 $\lambda(n)$.

We also have considered the somewhat easier problem of computing the average of $\ell_a(p)$ for a fixed integer a as p varies over primes. Here, because of Artin, we expect $\ell_a(p)$ to be of order p on average. But, what is the constant?

Kurlberg, P: *Assume the GRH. The average order of* $\ell_2(p)$ *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, $l_2(p) > \frac{4}{7}p$.

We have also worked out the constant where 2 is replaced with a general integer a, or even a general rational a. The details are a bit difficult because of “entanglements” in the Kummerian fields involved.

Here is the theorem we prove.

Kurlberg, P: *Let a be a rational number not equal to* $0, \pm 1$*. And let x be greater than both the numerator and denominator of a in absolute value. Assuming the GRH, we have uniformly*

$$\frac{1}{\pi(x)} \sum_{p \le x} \ell_a(p) = \frac{1}{2} c_a x + O\left(\frac{x}{(\log x)^{1/2-\epsilon}}\right).$$

Further, the constant c_a is identified as

$$c_a = \sum_{n=1}^{\infty} \frac{\varphi(n)\mathrm{rad}(n)(-1)^{\omega(n)}}{n^2 D_a(n)},$$

where $D_a(n)$ is the degree of the splitting field of $X^n - a$ over $\mathbb{Q}$.

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, On a problem of Arnold: the average multiplicative order of a given integer, arXiv.

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.

Thank You!