Order and chaos

Carl Pomerance, Dartmouth College
Hanover, New Hampshire, USA

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?

For an odd number n, let $l(n) = l_2(n)$ denote the mutliplicative order of 2 in $(\mathbb{Z}/n\mathbb{Z})^\times$. Note that

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

In fact, it is not hard to prove that the number of perfect shuffles to return a deck of $2n$ cards to it's initial order is $l(2n-1)$.

(Number the cards 0 to $2n-1$, with 0 the bottom card. Then a perfect shuffle takes a card in position i and sends it to $2i$ mod $(2n-1)$.)

This function $l(n)$ (= the multiplicative order of 2 mod n) appears to be very erratic and difficult to get hold of. It is of interest not only in card shuffling, but in computing the periods of certain pseudo-random number generators, and in other cryptographic contexts.

Further, as a basic and ubiquitous number-theoretic function it seems interesting to study $l(n)$, and more generally $l_a(n)$ (the order of a in $(\mathbb{Z}/n\mathbb{Z})^\times$) from a statistical viewpoint.

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

What is it normally?

What is it on average?

First, some number theory notation:

$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$

Thus, $l_a(n) \mid \varphi(n)$ when $(a, n) = 1$.

More notation:

We say $f(x) \sim g(x)$ as $x \to \infty$ if $\lim_{x \to +\infty} f(x)/g(x) = 1$.

$\pi(x)$ is the number of primes in $[1, x]$.

The Prime Number Theorem: $\pi(x) \sim x/\log x$ as $x \to \infty$.

One elementary result that goes back to Gauss and Carmichael is that $l_a(n) \mid \lambda(n)$.

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

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

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

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 n is prime.

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

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

where

$$A = \prod_p (1 - 1/p(p-1)) = 0.3739558136\ldots$$

is known as Artin's constant.

Let $P_a(x)$ denote the number of primes $p \leq x$ for which a is a primitive root for p. It is thus perhaps natural to conjecture that

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

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 $\mathbb{Q}(a^{1/n}, \zeta_n)$.

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

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

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 simple formula for $R(n)$. It is not so hard: For each prime $q \mid \lambda(n)$, let v_q be the exact exponent on q in the factorization of $\lambda(n)$, and let $\Delta_q(n)$ be the q-rank of

$$\left((\mathbb{Z}/n\mathbb{Z})^\times\right)^{q^{v_q-1}} \quad \text{(subgroup of } q^{v_q-1} \text{ powers)}.$$

With the numbers $\Delta_q(n)$ we can write down a formula for $R(n)$:

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

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 $\mathcal{R}(x)$ is chaotic. That is,

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

What's going on?

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 say $\log\log n$ is close to a power of 2, and another say, 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* $[0,1]$*.*

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 also was the subject of one the *Chern Lectures* he gave at UC Berkeley in 2007.

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 $l_a(n)$ 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 $l(n)$ $(= l_2(n))$ 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 $l(p) = p - 1$, so that just the contribution of primes to the sum of $l(n)$ 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".

Balazard, Kurlberg, 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.

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 $y \le (\log x)^{1-\varepsilon}$.)

Probably better suited for presentation in a talk is a proof of the following result from Balazard, Kurlberg, & P:

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

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

(Recall that $l(p) = l_2(p)$, the order of 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$.) Note that $\frac{159}{160}c = 0.57236022\ldots$, so that on average, $l(p) > \frac{4}{7}p$.

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

We are to prove that

$$\sum_{p\le x} l(p) \sim \frac{159}{320} cx\pi(x), \quad x \to \infty.$$

For an odd prime p, let $i(p) = (p-1)/l(p)$, namely the index of the subgroup $\langle 2\rangle$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. Let z be some parameter tending to infinity that we will specify later. We have

$$\sum_{p\le x} l(p) = \sum_{\substack{p\le x \\ i(p)\le z}} l(p) + \sum_{\substack{p\le x \\ i(p)>z}} l(p) = S + T,$$

say. Further, if $z \le \log x/\log\log x$, then the Kurlberg–P lemma implies

$$T = O\left(\frac{x}{z}\cdot\frac{\pi(x)}{z}\right),$$

which is $o(x\pi(x))$ provided $z \to \infty$.

Now, for the main term S we might use known results for the distribution of primes p where $i(p)$ is fixed at some number, but it seems simpler to use an inclusion–exclusion:

$$S = \sum_{\substack{p \le x \\ i(p) \le z}} (p-1) \sum_{uv | i(p)} \frac{\mu(v)}{u}.$$

Here μ is the Möbius function. It encodes the principle of inclusion-exclusion from combinatorics and is defined:
$\mu(v) = 0$ if v is not squarefree and
$\mu(v) = (-1)^k$ when v is squarefree and has k prime factors.

We write $S = U - V$, where in U we drop the condition $i(p) \le z$, but assume $uv \le z$, while in V we assume that $i(p) > z$ and $uv \le z$.

We have

$$V = \sum_{\substack{p \le x \\ i(p) > z}} (p-1) \sum_{\substack{uv \mid i(p) \\ uv \le z}} \frac{\mu(v)}{u}.$$

We majorize trivially by replacing $\mu(v)$ with 1. For $z < i(p) < z^2$, the number of choices of v is $z^{o(1)}$, so the inner sum is at most $z^{o(1)}$, and the contribution to V is at most $x\pi(x)/z^{1-o(1)}$.

When $i(p) \ge z^2$, the number of choices of v is at most z/u, so the inner sum is $O(z)$ and the contribution to V is at most $O(x\pi(x)/z)$ provided $z \le (\log x/\log\log x)^{1/2}$.

This leaves the main term

$$U = \sum_{p \le x} (p-1) \sum_{\substack{uv \mid i(p) \\ uv \le z}} \frac{\mu(v)}{u} = \sum_{uv \le z} \frac{\mu(v)}{u} \sum_{\substack{p \le x \\ uv \mid i(p)}} (p-1).$$

For a given value of $uv \le z$, we can compute the inner sum by partial summation and a GRH-conditional result in Hooley, getting

$$\frac{x\pi(x)}{2uv\varphi(uv)} + O\left(\frac{x\pi(x)}{\log x}\right)$$

if $8 \nmid uv$ and twice this if $8 \mid uv$. (If $z \le (\log x)^{1/7}$, say, we have this unconditionally, but we needed the GRH to estimate the error term V.)

Thus, the main term is

$$U = \frac{1}{2} x\pi(x) \left(\sum_{uv \le z} \frac{\mu(v)}{u^2 v \varphi(uv)} + \sum_{\substack{uv \le z \\ 8 | uv}} \frac{\mu(v)}{u^2 v \varphi(uv)} \right) + O\left(\frac{x\pi(x) z \log z}{\log x} \right).$$

So we see that a convenient choice of z is $(\log x / \log\log x)^{1/2}$. For the main term, we consider the expressions as infinite sums, estimate the errors in truncation, and then rewrite the infinite sums as Euler products. We get:

$$\frac{1}{\pi(x)} \sum_{2 < p \le x} l(p) = \frac{159}{320} cx + O\left(\frac{x}{(\log x)^{1/2-\varepsilon}} \right).$$

□

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.

M. Balazard, 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, to appear.