ORDER AND CHAOS

Carl Pomerance, Dartmouth College

Hanover, New Hampshire, USA

Hudson River Undergraduate Mathematics Conference

April 16, 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 and the top card staying on the top).

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.

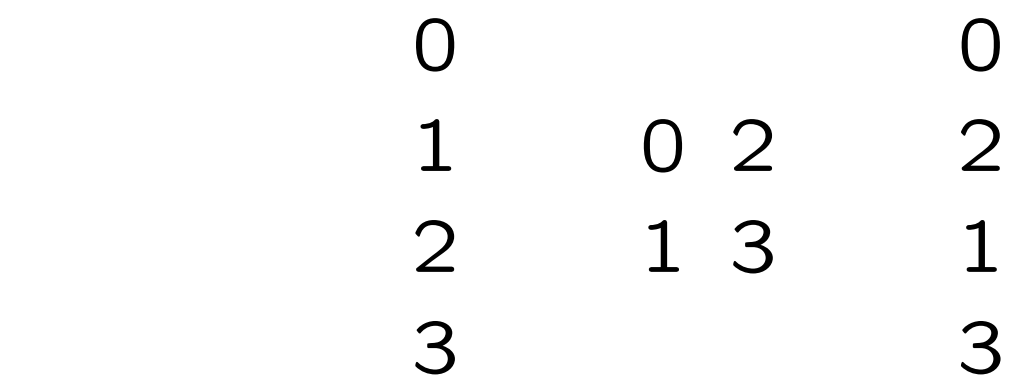
Do you believe me? And what's going on?

Persi Diaconis

Lets try it out for smaller decks. Say 4 cards.

Number the 4 positions in the deck 0, 1, 2, 3, where 0 is the postion for the top card, 1 is the position for the second card, and so on. (This is the way computer scientists count, and the way floors are numbered in Europe.)

And here's one shuffle:



So doing one perfect shuffle on a deck of 4 cards just reverses the two middle cards, so doing it twice would return the deck to its original order.

Lets try 6 cards. Here are two shuffles:

0			0			0		
1	0	3	3	0	4	4		
2	1	4	1	3	2	3		
3	2	5	4	1	5	2		
4			2			1		
5			5			5		

Two shuffles reverse the order of the middle 4 cards, so four shuffles would return this deck to its starting order.

Lets try 8 cards:

0		0		0		0	
1	0 4	4	0 2	2	0 1	1	
2	1 5	1	4 6	4	2 3	2	
3	2 6	5	1 3	6	4 5	3	
4	3 7	2	5 7	1	6 7	4	
5		6		3		5	
6		3		5		6	
7		7		7		7	

So, with 8 cards, it takes 3 shuffles.

And now lets try to see what's happening with $2n$ cards. Here's one shuffle:

0	0	n	0
1	1	$n+1$	n
2	2	$n+2$	1
3	3	$n+3$	$n+1$
4	4	$n+4$	2
⋮	⋮	⋮	⋮
$2n-2$	$n-2$	$2n-2$	$n-1$
$2n-1$	$n-1$	$2n-1$	$2n-1$

Is there some simple way to explain in a formula what happens to the card in position i after one shuffle?

0	0	n	0
1	1	$n+1$	n
2	2	$n+2$	1
3	3	$n+3$	$n+1$
4	4	$n+4$	2
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$2n-2$	$n-2$	$2n-2$	$n-1$
$2n-1$	$n-1$	$2n-1$	$2n-1$

So, the card in position 0 goes to position 0, the card in position 1 goes to position 2, and so on. For the first half the card in position i goes to position $2i$.

In the second half of the deck: The card in position $n + i$ goes to position $2i + 1$, which we could write as $2(n + i) - (2n - 1)$.

Arithmetic modulo m:

Here m is a positive integer. We do ordinary arithmetic except when we get the answer, we divide by m and get the remainder.

With $m = 2n - 1$, we have that one perfect shuffle on a deck of $2n$ cards sends a card in position i to position $2i \bmod m$. (This

formula doesn't quite work for the bottom card, but we know this card stays fixed.)

So, a perfect shuffle just doubles the position number, as long as we remember to keep these numbers in our range by dividing by $2n - 1$ and getting the remainder.

Let $S(i)$ be the position that a card in position i gets sent to after one perfect shuffle. We have figured out that

$$S(i) \equiv 2i \pmod{2n-1}.$$

So, if we do two shuffles, we have

$$S^{(2)}(i) = S(S(i)) \equiv 2^2 i \pmod{2n-1}$$

and in general after k shuffles,

$$S^{(k)}(i) \equiv 2^k i \pmod{2n-1}.$$

We're in the home stretch: We just need to find the least number k with

$$2^k \equiv 1 \pmod{2n-1}.$$

What are the powers of 2 modulo 51? They are

$$2,\ 4,\ 8,\ 16,\ 32,\ 13,\ 26,\ 1,$$

so we have

$$2^8 \equiv 1 \pmod{51}$$

and this explains the 8 perfect shuffles for a deck of 52 cards.

Here's a question: Given a deck of size $2n$ are we sure there will be *some* number of perfect shuffles to return it to its order? That is, are we sure that there is *some* positive integer k with

$$2^k \equiv 1 \pmod{2n-1} \ ?$$

Well, Euler says 'yes.' For a positive integer m, let $\varphi(m)$ be the number of integers in $\{1, 2, \ldots, m\}$ that are relatively prime to m. For example, $\varphi(3) = 2$, $\varphi(10) = 4$, $\varphi(51) = 32$.

Euler: If the integer a is relatively prime to m, then

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Leonhard Euler

We are looking at the **order function**. If a, m are relatively prime, let $l_a(m)$ denote the order of a modulo m, namely the smallest positive integer k with $a^k \equiv 1 \pmod{m}$.

From Euler, we know that $l_a(m)$ exists, and in fact, it is not hard to show that $l_a(m) \mid \varphi(m)$.

Here are some values with $a = 2$, so that it corresponds to shuffling:

$l_2(47) = 23$, $l_2(49) = 21$, $l_2(51) = 8$, $l_2(53) = 52$

$l_2(123) = 20$, $l_2(125) = 100$, $l_2(127) = 7, \ldots$

When a small change in input can produce a large change in output, we are looking at

a *chaotic* function. This function $l_2(m)$ for odd numbers m appears to be 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) $= 4$

$$\mathrm{Peri}(103) = 34$$

$$\mathrm{Peri}(107) = 53$$

$$\mathrm{Peri}(109) = 108$$

$$\mathrm{Peri}(111) = 3$$

$$\mathrm{Peri}(113) = 112$$

For numbers m relatively prime to 10, Peri$(m) = l_{10}(m)$, so again we have an order function, and again it is chaotic.

We have seen in these examples that the order function $l_a(n)$ is chaotic, thus explaining the title of this lecture.

The order function has applications in cryptography and in computing the periods of certain pseudo-random number generators. In fact, the RSA cryptosystem relies for its security on the difficulty in computing the order function.

The Blum–Blum–Shub pseudo-random number generator: Start with a positive integer m and a "seed" s, and let

$$x_j = s^{2^j} \bmod m,$$

for $j = 0, 1, \ldots$. To go from x_j to x_{j+1} one just squares, divides by m, and takes the remainder. Often this is done with m the product of two large prime numbers, and

one creates a stream of 0's and 1's based on whether x_j is even or odd.

This is not really random, and in fact it will eventually be periodic. Say the largest odd divisor of $l_s(m)$ is d. Then the period length is $l_2(d)$.

In the RSA cryptosystem, one has a number m that is the product of two large primes and two numbers E and D with $ED \equiv 1 \pmod{\varphi(m)}$. If M is a message that is a number in the range 0 to $m-1$, then the encrypted form of the message is

$$X = M^E \bmod m.$$

The question is if one can easily retrieve M from knowing X. If you know the secret

decryption number D, then yes, since

$$M = X^D \bmod m.$$

If you could compute $\varphi(m)$ (which is essentially equivalent to factoring m), one could compute D from knowing E.

But if you could compute orders, you'd be just as happy. Say you could compute $l_X(m)$, call it F. It is easy to come up with a number D' with $ED' \equiv 1 \pmod{F}$. And then

$$M = X^{D'} \bmod m.$$

Like computing $\varphi(m)$, computing orders is essentially as hard as computing the prime factorization of the modulus m, and we know no way to routinely factor large numbers. That is, on conventional computers.

Quantum computers theoretically can compute orders very easily. Except it is not so easy to build a quantum computer!

How might one "tame" a chaotic function? One way is to look at it statistically. Lets take as an example, the function $\omega(n)$, the number of primes that are divisors of n.

For example, $\omega(10) = 2$, $\omega(11) = 1$, $\omega(12) = 2, \ldots$. It does not look very chaotic!

However, there is chaos, just a more gentle variety. Consider for example that

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

It is easy to show that on average, $\omega(n)$ behaves like $\log\log n$. (In number theory we use 'log' for the natural logarithm.) That is,

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

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).

G. H. Hardy

S. Ramanujan

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

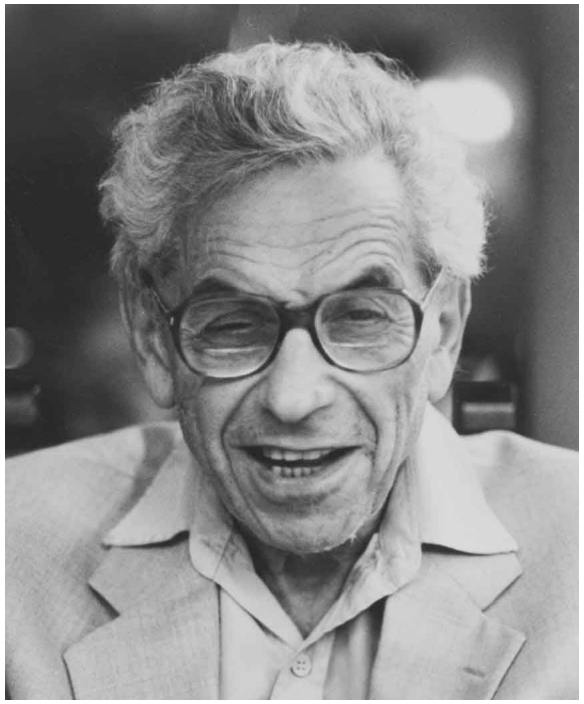
$$\omega(n) \leq \log\log n + u\sqrt{\log\log n}$$

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

There is some famous work concerning $l_a(p)$ where p is a prime not dividing the integer a. We know that $l_a(p) \mid \varphi(p)$ and that $\varphi(p) = p - 1$. We also know that there are choices for a where $l_a(p) = p - 1$.

For example, with $a = 2$ and $p = 53$. That's why it takes a whopping 52 perfect shuffles for a deck of 54 cards.

Another example is with $a = 10$ and $p = 109$. That's why the length of the repeating period for the decimal expansion of $1/109$ is a whopping 108.

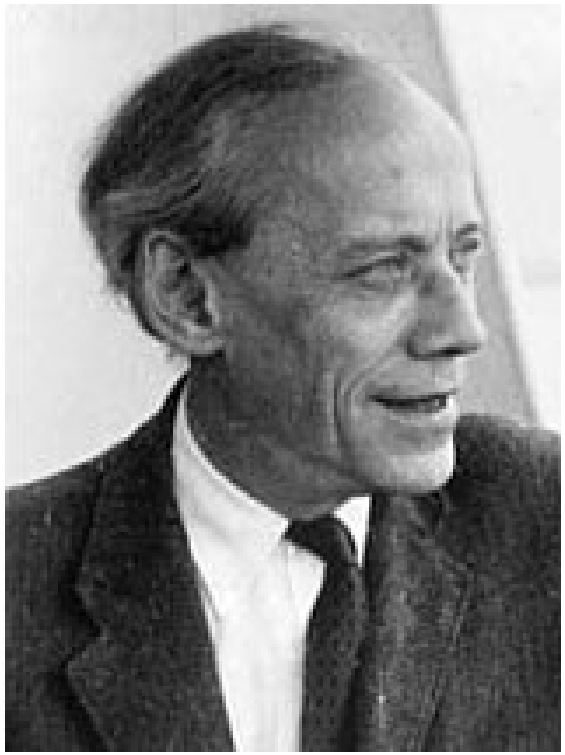
Over two centuries ago, Gauss asked if this deal with the decimal for $1/p$ occurred for infinitely many primes p. I.e., do we have $l_{10}(p) = p - 1$ for infinitely many primes p?

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 $l_a(p) = p - 1$ 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 $l_a(p) = p - 1$. (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. In general, let $\lambda(n)$ denote the largest possible value of $l_a(n)$ as a varies over numbers relatively prime to n. We always have $\lambda(n) \mid \varphi(n)$, and when n is prime, they are equal. But most of the time $\lambda(n)$ is much smaller than $\varphi(n)$. For example, $\varphi(91) = 72$ but $\lambda(91) = 12$.

A natural generalization of the Gauss–Artin problem:

For a fixed integer a outside of some sparse exceptional set, do we have $l_a(n) = \lambda(n)$ 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

It is easy to come up with sets of numbers which do not have an asymptotic density. For example, take the numbers with an even number of digits.

It is a bit of a surprise though when oscillations occur in non-artificial situations. Where does the oscillation come from in considering the frequency of numbers n with $l_a(n) = \lambda(n)$?

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.

When we're faced with very hard problems, sometimes a way of getting some partial information is to consider the situation on average. In the two situations we've just looked at, we were considering extreme values of $l_a(p)$ and $l_a(n)$ for a given a.

We could instead study the average values of these functions of p or n. One too could consider the average as a function of a or over both variables. For example, Luca worked out the asymptotic behavior of

$$\sum_{p \leq x} \sum_{a=1}^{p-1} l_a(p)$$

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

Florian Luca

Yilan Hu

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

After some numerical experiments, he concluded that

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

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.

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 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 $l_a(n)$. 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.

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

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

What this question means is: How does

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

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.

The extra factor tends to infinity more slowly than any fixed power of $\log x$.

Eric Schmutz

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 $x/\log x$ is supported on

one side by Hooley's GRH-conditional proof of Artin's conjecture. (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 of the shape $x/\log x$.) And perhaps $l_a(n)$ is sufficiently small for composite numbers n, that these do not contribute too much. Further, perhaps the

average order of $\lambda(n)$ is not that relevant, since this average is supported on a thin set of numbers n with abnormally large λ values, and the behavior for $l_a(n)$ may be markedly different.

However...

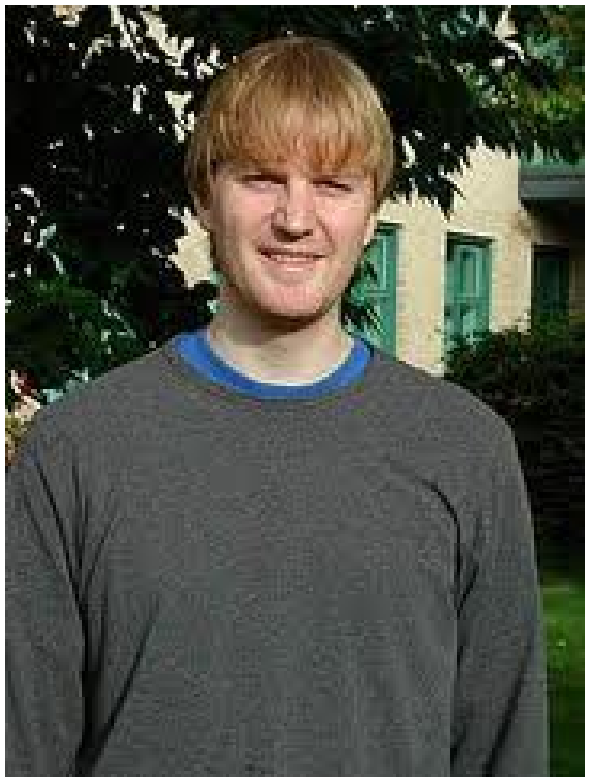
Kurlberg and P: *Let* $|a| > 1$. *Assuming the Generalized Riemann Hypothesis,*

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

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

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

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 $\lambda(n)$.

Perhaps it is better to end now, and reflect how the innocent problem of perfect shuffles has led all this way.

THANK YOU!

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.