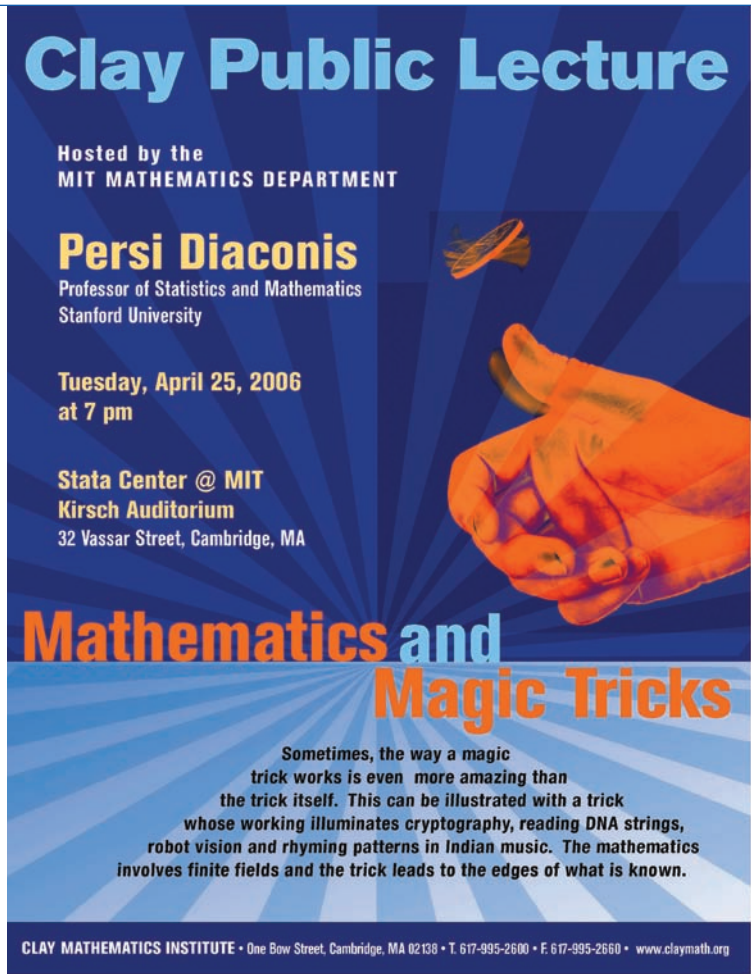
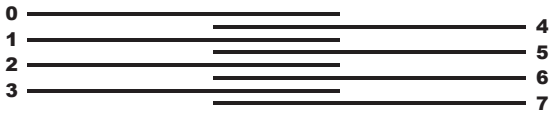
Mathematics and Magic Tricks

Persi Diaconis
Department of Mathematics and Statistics
Stanford University



The way that a magic trick works can be just as amazing as the trick itself. My favorite way of illustrating this is to talk about shuffling cards. In this article, I will try to explain how there is a direct connection between shuffling cards and the Riemann Hypothesis — one of the Clay Mathematics Institute's Millennium Prize Problems.

Let us begin with perfect shuffles. Magicians and gamblers can take an ordinary deck of cards, cut it exactly in half, and shuffle the two halves together so that they alternate perfectly as in figure one, which shows a perfect shuffle of an eight-card deck.



If the shuffle is repeated eight times with a fifty-two card deck, the deck returns to its original order. This is one reason that perfect shuffles interest magicians. To see why gamblers are interested, suppose that the deck begins with four aces on top. After one perfect shuffle, the top of the deck is Ace, X, Ace, X, Ace, X, Ace, X, where X is an indifferent card. After two perfect shuffles, the aces are four cards apart. Thus, if four hands of poker are dealt, the dealer's accomplice gets the aces. This motivates the study of just what can be done with perfect shuffles. Magicians and gamblers (along with a few mathematicians) have been thinking about such things for at least three hundred years.

To see the connections with mathematics, consider the problem of how many times a deck should be shuffled to recycle it. The answer is eight for a fifty-two card deck. The answer is fifty-two for a fifty-four card deck and six for a sixty-four card deck. The number of perfect shuffles needed to recycle various size decks is shown in table one.

deck size $2n$	2	4	6	8	10	12	14	16	18	20	22	24	26	
$ord_2(2n-1)$	1	2	4	3	6	10	12	4	8	18	6	11	20	
deck size $2n$	28	30	32	34	36	38	40	42	44	46	48	50	52	54
$ord_2(2n-1)$	18	28	5	10	12	36	12	20	14	12	23	21	8	52

Can the reader see any pattern in these numbers? Some people find it surprising that sometimes larger decks recycle after fewer shuffles. Decks that have size power of two can be seen to recycle particularly fast. To understand this better, label a deck of size $2n$, starting from the top, as 0, 1, 2, 3, ..., $2n$ - 1. Observe that after one perfect shuffle, the card in position i moves to position $2i$. This statement is true even when i is greater than $n/2$, provided we take the remainder of $2i$ when divided by $2n$ - 1. Or, as mathematicians say, we compute $2i$ modulo $2n$ - 1. Thus, when $2n = 52$, the card in position 0 stays there. The card in position 1 moves to position

2 (because we label things starting at zero, position 2 means the third card from the top). The card in position 28 goes to position 56 modulo 51, that is, to position 5. And so on.

Returning to the problem of a deck of arbitrary size n, we see that after one shuffle, card i moves to position $2i$ modulo $(2n - 1)$. After two shuffles, it moves to position $4i$ modulo $(2n - 1)$. After three shuffles, it moves to position $8i$ modulo $(2n - 1)$. Therefore, the deck recycles after k shuffles, where k is the smallest power of two such that 2 raised to the kth power is one modulo $2n - 1$. For example, when $2n = 52$, $2n - 1 = 51$, and the various powers of two modulo $2n - 1$ are

0 2 4 8 16 32 13 26 1

That is, $2^8 = 256 = 1$ modulo 51, so fifty-two cards recycle after eight shuffles. For a fifty-four card deck, 2 raised to the power 52 is 1 modulo 53. One sees that fifty-two shuffles, but no fewer, are required. For a sixty-four card deck, 2 raised to the power 6 is 1 modulo 63. One sees that in six shuffles, but no fewer, the deck is recycled.

Persi Diaconis delivering his talk at MIT.

From these observations, it is natural to wonder what the longest recycling times are. Fermat's little theorem shows that the worst that can happen is that the deck recycles after $2n - 2$ shuffles. Does this happen for arbitrarily large decks? No one knows. It is a conjecture, due to Emil Artin, with antecedents in the work of Gauss, that 2 is a primitive root for arbitrarily large primes. (See [1, 6] and [3, 4]). This would yield an affirmative answer to the card shuffling problem. It has been rigorously proved that if the generalized Riemann Hypothesis holds, then the Artin conjecture holds. But, alas, a proof of the Riemann Hypothesis, even in its original form, continues to elude the efforts of the world's mathematicians.

The audience assisting in one of Persi's tricks.

I find these connections wonderful. It is inspiring, indeed awe-inspiring, that a simple card-shuffling question that fascinated me as a kid of thirteen can lead to the edge of mathematics and beyond. If you want to know more about shuffling cards and its connections to all sorts of mathematics, see [2].

References

1. Artin, E., letter to Helmut Hasse, September 27, 1929. Recorded in the diary of Helmut Hasse.

2. Diaconis, P. and Graham, R.L. (2007) "The Solutions to Elmsley's Problem." *Math Horizons*, Feb. 2007, pg. 22 - 27. See maa.org.

3. Gauss, C-F., *Disquisitiones Arithmetica*, articles 315-317. 1801.

4. Li, Shuguang and Pomerance, C., *Primitive roots: a survey*, http://www.math.dartmouth.edu/~carlp/PDF/primitiverootstoo.pdf

5. Moree, P., Artin's primitive root conjecture, http://www.math.tau.ac.il/~rudnick/dmv/moree.ps

6. Wikipedia, Artin's conjecture on primitive roots, http://en.wikipedia.org/wiki/Artin's_conjecture_on_primitive_roots