A standard deck of cards consists of 52 cards: four suits of 13 cards each. Before playing a game one wants to ensure that the cards have been shuffled: that some procedure has been carried out to put the cards in an unpredictable order. One way of doing this is to repeatedly riffle shuffle the cards.

Deck of cards Two stacks after cutting

To riffle shuffle, first cut the deck and then randomly choose a stack from which to choose the bottom card and place in the new deck. (One could toss a coin to decide each time which stack to remove the bottom card from; in practice this is done by "riffling" or "dovetailing" the cards.)

A perfect riffle shuffle is when the deck is cut in half and one alternates taking bottom cards from one stack and then the other. No randomness is involved. A perfect riffle is very difficult, but not impossible, to do by hand. If we perform perfect riffle shuffles, will we get a deck that is not predictable?

Example (Perfect Riffle) Number the cards from 0 to 51 with 0 on top.

0					0
1		0	26		26
2	Cut in half	1	27	Perfect riffle (right first)	1
3		2	28		27
⋮		⋮	⋮		⋮
50		24	50		24
51		25	51		50
					25
					51
Numbered deck		Two stacks			Perfect riffle shuffle

The cards in positions $0, 1, 2, \ldots, 25$ have moved to positions $0, 2, 4, \ldots, 50$ while the cards in positions $26, 27, \ldots, 51$ have moved to positions $1, 3, 5, \ldots, 49, 51$. Every card has moved from position j to position $2j \bmod 51$. The perfect riffle shuffle is entirely predictable! Moreover, if we perform two perfect riffle shuffles in a row, the card in position j will move to position $4j \bmod 51$.

Original position	j
After 1 perfect riffle	$2j \bmod 51$
— 2 —	$4j \bmod 51$
— 3 —	$8j \bmod 51$
— 4 —	$16j \bmod 51$ ~~13 mod 51~~
— 5 —	$32j \bmod 51$
— 6 —	$64j \bmod 51 = 13 \bmod 51$
— 7 —	$26j \bmod 51$
— 8 —	$52j \bmod 51 = j \bmod 51$

After eight perfect riffle shuffles the card from position j is back to position j. The deck has not been shuffled at all! $\square$

Performing perfect riffle shuffles is <u>not</u> a good way to shuffle a deck! There are only eight possible rearrangements of the original deck that one could ever get as a result of repeatedly riffle shuffling perfectly.

A riffle shuffle is not so predictable: we have 51 choices for the cut and, cutting above card j, we have $\binom{52}{j}$ possible outcomes for the riffle. That gives at most

$$\sum_{j=1}^{51} \binom{52}{j} = 2^{52} - 2$$

possible outcomes from a single riffle shuffle. (Some riffle shuffles give the same outcome.) This seems like a lot: $2^{52} - 2 \approx 10^{15}$ outcomes. But there are $52!$ arrangements of 52 playing cards!

$$52! \approx 10^{68}$$

is a very large number. After one riffle shuffle we can only arrive at a microscopic (in fact, less than a queccascopic) fraction of all arrangements.

Questions

How many riffle shuffles should be performed to guarantee a shuffled deck?

How do we choose where to cut? (A cut close to the middle seems more likely.)

How is the randomness of the riffle best described? (More likely to pull from the bigger stack?)

It turns out (as we shall see at the end of the course) that seven riffle shuffles is enough, but six is not.