Card Shuffles

I put a pack of eight cards on the table. The top card has an A written on it. The next card has a B written on it, etc

I pick up the top half of the pack, A, B, C, D in my right hand.

I pick up the bottom half of the pack, E, F, G, H in my left hand.

Then I do a riffle shuffle:

I drop the D card from my right hand onto the table, then the H card from my left hand, then the C card from my right hand, then the G card from my left hand, then the B card from my right hand, then the F card from my left hand, then the A card from my right hand, then the E card from my left hand.

The cards are now in the order E, A, F, B, G, C, H, D with the E on the top of the pile. Try it.

Then I shuffle again and again until the cards are back in their original order.

So how have the cards moved?

Order at start	A	B	C	D	E	F	G	H
Order after one shuffle	E	A	F	B	G	C	H	D
Order after two shuffles	G	E	C	A	H	F	D	B
Order after three shuffles	H	G	F	E	D	C	B	A
Order after four shuffles	D	H	C	G	B	F	A	E
Order after five shuffles	B	D	F	H	A	C	E	G
Order after six shuffles	A	B	C	D	E	F	G	H

So the cards are back in their original order after six shuffles.

It will be helpful to look at the position of each card in the pack. Position 1 is the top card etc

Card	A	B	C	D	E	F	G	H
Position at start	1	2	3	4	5	6	7	8
Position after one shuffle	2	4	6	8	1	3	5	7
Position after two shuffles	4	8	3	7	2	6	1	5
Position after three shuffles	8	7	6	5	4	3	2	1
Position after four shuffles	7	5	3	1	8	6	4	2
Position after five shuffles	5	1	6	2	7	3	8	4
Position after six shuffles	1	2	3	4	5	6	7	8

You can check that:

After 1 shuffle, the card starting in position m will end up in position $2m, mod\, 9$

After 2 shuffles, the card starting in position m will end up in position $(2\times2)m, mod\, 9$

After 3 shuffles, the card starting in position m will end up in position $(2\times2\times2)m, mod\, 9$

...

After k shuffles, the card starting in position m will end up in position $2^k m, mod\, 9$

If $2^k m=m, mod\, 9$ for $m=1,2,...8$ then after k shuffles, the card starting in position m will end up in position m So the cards are back in their original order.

Now $2^6=1, mod\, 9$ You can check this.

So $2^6\times1=1, mod\, 9$ and $2^6\times2=2, mod\, 9$ and $2^6\times3=3, mod\, 9$ and … $2^6\times8=8, mod\, 9$

So the pack of 8 cards will be back in their original order after 6 shuffles.

In general:

Take a pack of N cards:

If $2^k=1, mod(N+1)$ then the cards will be back in their original order after k shuffles.

We know from Fermat’s little theorem that:

$2^{(p-1)}=1, mod\, p$ provided $p\neq2$

So:

Take a pack of $p-1$ cards: where p is a prime number

Now $2^{(p-1)}=1, mod\, p$ so the cards will be back in their original order after p shuffles.

A pack of 52 cards will be back in its original order after 52 shuffles, because 53 is prime.