SHUFFLING CARDS

Amy Suo
amysuwoah@gmail.com
Senjuti Dutta
senjutid58@gmail.com
Alex Arnell
alexandergarnell@gmail.com

Counselor: Natalie Merson

August 2, 2019

Contents

1 Introduction

Shuffling cards has become a part of our daily lives whether its playing fish with our friends or performing magic tricks in shows. Card shuffling has become one of the most (adj) arts through the smooth feel of a riffle or the beautiful patterns of the cards. However, many people disregard the almost magical mathematical properties of card shuffling.

Some of the most important questions are how efficient is the shuffling? Is repeated shuffling a good idea? What is the worst number of shuffles?How many times should we shuffle to get the best possible results?

Definition 1 (Perfect shuffle) *We define a 'perfect' shuffle as the following: Take a stack of m playing cards, with m even, cut it into two equal stacks, and place one on the left and one on the right alternately select the top card from each stack of $\frac{m}{2}$ cards, left then right then left then right and so on, and place in turn each newly selected card below those selected previously till you end up with a reordered stack of cards of the original stack.*

There are a few kind of shuffles like top-up, top-down, bottom-up, bottom-down. However the main types of shuffles(in practice) are top-up and bottom-up.

Definition 2 (Top shuffle) *During a shuffle, after cutting the deck into two equal stacks, if we take the first card from the top half of the deck first, then it is called top shuffle.*

Definition 3 (Bottom shuffle) *During a shuffle, after cutting the deck into two equal stacks, if we take the first card from the bottom half of the deck first, then it is called bottom shuffle.*

Definition 4 (Up shuffle) *During a shuffle, after cutting the deck into two equal stacks, we can either take a card from the top or bottom of each stack. The shuffle is considered a up shuffle if every time we select a new card, we take it from the top of the deck.*

Definition 5 (Down shuffle) *During a shuffle, after cutting the deck into two equal stacks, we can either take a card from the top or bottom of each stack. The shuffle is considered a down shuffle if every time we select a new card, we take it from the bottom of the deck.*

2 Period of Cards

Now there are many remarkable properties of these shuffles. One of the amazing property is that if you take a deck of 52 cards and shuffle it 8 times, it returns back to its original order of cards. Some of the questions that arise are is this something special? Is it something common and expected? Is 52 a special number? Does this happen to other number of cards as well? Let us take some time to understand the reason behind such phenomenon.

For our convenience and simplicity, we are numbering each card according to their order. So a deck of 52 cards would have numbers from 1 to 52 on each one of them and the starting deck (before shuffling) is the deck containing cards in order of their numbers with 1 being on the top.

If we do a top shuffle on a deck of 52 cards 8 time continuously, the deck would look something like this: (insert the data....the shuffles).

Definition 6 (Period) *The least number of times a deck of cards is shuffled perfectly in order to revert back to the original position it started in is called the period of the shuffle.*

So the period of 52 is 8. Now let us look at the period of some other number of cards.

3 Two Handed Shuffles

3.1 Top Up Shuffle

Now is a good time for us to come up with some conjectures.

Conjecture 1 *For top shuffle, the period of 2^{2k} is $2k$ and the period of 2^{2k+1} is $2(2k+1)$, where $k \in \mathbb{Z}$.*

It does not seem like we have enough tools to prove this conjecture. So let us keep this aside for a moment and try to build our understanding.

Definition 7 *$f : \mathbb{Z} \to \mathbb{Z}$ is the position of a card after a shuffle. For example $f(n)$ is the position of the n^{th} card after shuffling once.*

Definition 8 *Given $a, m \in \mathbb{N}$ such that $(a, m) = 1$, then $n \in \mathbb{N}$ is called the order of a mod m if*

$$a^n \equiv 1 \pmod{m}$$

Theorem 1 *For $n \in \mathbb{N}$, n is even, let the order of 2 mod (n-1) be m. Then for a top shuffle, the period for n cards (n is even) is*
m , if m is even or
$2m$, if m is odd.

Proof: Let $n \in \mathbb{N}$, n is even, be the total number of cards.

Claim 1: For $x \in \mathbb{Z}$

$$f(x) = \begin{cases} n + 2 - 2x, & \text{if } x \leq \frac{n}{2} \\ 2n + 1 - 2x, & \text{if } \frac{n}{2} < x \leq n \end{cases}$$

Proof of claim: we would prove it by induction. Let there be n cards.

Base case: Since it is the top shuffle, so the first card would go to the bottom. Hence, $f(1) = n$ and $f(\frac{n}{2} + 1) = (n - 1)$.

Induction hypothesis: Let for $k \in \mathbb{N}$,

$$f(k) = \begin{cases} n + 2 - 2k, & \text{if } k \leq \frac{n}{2} \\ 2n + 1 - 2k, & \text{if } \frac{n}{2} < k \leq n \end{cases}$$

Now for $(k + 1)$ if both k and $k + 1$ are in the same stack, then after shuffling, one card from the other stack goes between the k^{th} and $(k + 1)^{th}$ card. Hence

$$f(k+1) = f(k) - 2 = \begin{cases} n + 2 - 2(k + 1), & \text{if } (k + 1) \leq \frac{n}{2} \\ 2n + 1 - 2(k + 1), & \text{if } \frac{n}{2} < (k + 1) \leq n \end{cases}$$

If k and $(k + 1)$ are in different stacks then $k = \frac{n}{2}$. Then $(k + 1) = \frac{n}{2} + 1$. And we know $f(k + 1) = f(\frac{n}{2} + 1) = n - 1$.

Hence it is true for $(k + 1)$ whenever it is true for k and the base cases are already true. So

$$f(x) = \begin{cases} n + 2 - 2x, & \text{if } x \leq \frac{n}{2} \\ 2n + 1 - 2x, & \text{if } \frac{n}{2} < x \leq n \end{cases}$$

This is the end of proof of our claim.

Now notice that

$$f(x) \equiv \begin{cases} 3-2x, & \text{if } x \leq \frac{n}{2}, \quad (mod \quad (n-1)) \\ 3-2x, & \text{if } \frac{n}{2} < x \leq n \quad (mod \quad (n-1)) \end{cases}$$

Hence $f(x) \equiv 3-2x \quad (mod \quad n-1)$.

Now let $m \in \mathbb{N}$ be the period of the shuffle. So after m shuffles the positions of each card should be its initial position. Hence $f^m(x) = x(mod \quad (n-1))$.

Claim 2: For $m \in \mathbb{N}$, $f^m(x) = 3(1-2+...+(-1)^{m-1}.2^{m-1}) + (-1)^m 2^m x$.

Proof: We would prove it by induction.

Base case: for $k=1$, $f(x) = 3-2x = 3((-1)^0 2^0) + (-1)^1 2^1 x$. Hence it is true for the base case.

Induction hypothesis: Let for $k \in \mathbb{N}$, $f^k(x) = 3(1-2+...+(-1)^{k-1}.2^{k-1}) + (-1)^k 2^k x$.

Hence for $k+1$,

$$f^{k+1}(x) = 3(1-2+...+(-1)^{k-1}2^{k-1}) + (-1)^k 2^k (f(x))$$

$$= 3(1-2+...+(-1)^{k-1}2^{k-1}) + (-1)^k 2^k (3-2x)$$

$$= 3(1-2+...+(-1)^{k-1}2^{k-1} + (-1)^k 2^k) + (-1)^{k+1} 2^{k+1} x$$

So it is true for $k+1$ whenever it is true for k and it is true for base cases, so it is true for all $k \in \mathbb{N}$.

So $f^m(x) \equiv 3(1-2+...+(-1)^{m-1}.2^{m-1}) + (-1)^m 2^m x$

$$\equiv -3(2-1+2^3-2^2+...+2^{m-1}) + (-1)^m 2^m x$$

$$\equiv -3(1+2^2+...+2^{m-1}) + (-1)^m 2^m x$$

$$\equiv -(2^m-1) + (-1)^m 2^m x$$

$$\equiv 1-2^m+2^m x$$

Or $f(x) \equiv 1-2^m+2^m x$.

So m is the period if $f^m(x) \equiv x \quad (mod \quad (n-1))$ for all $x \in \mathbb{N}, \quad x \leq n$.

$$\implies 1-2^m+2^m x \equiv x \quad (mod \quad (n-1))$$

$$\implies 1-2^m \equiv x(1-2^m) \quad (mod \quad (n-1))$$

Since x is a variable position so,

$$2^m \equiv 1 \quad (mod \quad (n-1))$$

So if α is the order of 2 mod $(n-1)$ then the period :

$$m = \begin{cases} \alpha, & \textbf{if} \quad \alpha \quad \textbf{is even} \\ 2\alpha, & \textbf{if} \quad \alpha \quad \textbf{is odd} \end{cases}$$

□

Now we can go back to our conjecture.

Conjecture 1: For top shuffle, the period of 2^{2k} is $2k$ and the period of 2^{2k+1} is $2(2k+1)$, where k $\in \mathbb{Z}$.

Proof:Let $k, n \in \mathbb{N}$. We know that the period of n cards is the order of $2 \quad (mod \quad n)$, if the order is even. Let $n = 2^{2k}$, and let $m \in \mathbb{N}$ be the order of 2 (mod n). So $2^m \equiv 1 \quad (mod \quad 2^{2k} - 1)$

$$\implies 2^{2k} - 1 | 2^m - 1$$

$$\implies 2^{2k} - 1 \leq 2^m - 1 \tag{1}$$

Also since $2^{2k} \equiv 1 \quad (mod \quad (n-1))$ and m is the order so $m \leq 2k$. So $2^m \leq 2^{2k}$

$$\implies 2^m - 1 \leq 2^{2k} - 1 \tag{2}$$

Hence by trichotomy, and (1) and (2), we get that the order is $m = 2k$. Now since the order is even, so the period of 2^{2k} is $2k$.

Similarly, Let $n = 2^{2k+1}$, and let $m \in \mathbb{N}$ be the order of 2 (mod n). So $2^m \equiv 1 \quad (mod \quad 2^{2k+1} - 1)$

$$\implies 2^{2k+1} - 1 | 2^m - 1$$

$$\implies 2^{2k+1} - 1 \leq 2^m - 1 \tag{3}$$

Also since $2^{2k+1} \equiv 1 \quad (mod \quad (n-1))$ and m is the order so $m \leq 2k+1$. So $2^m \leq 2^{2k+1}$

$$\implies 2^m - 1 \leq 2^{2k+1} - 1 \tag{4}$$

Hence by trichotomy, and (3) and (4), we get that the order is $m = 2k+1$. Now since the order is odd, so the period of 2^{2k+1} is $2(2k+1)$. □

3.2 Bottom Up Shuffle

Recall *Definition 3* and *definition 4*. Since we now know what top-up shuffle is and its period, there are few questions that should be asked. Does top-up shuffle and bottom-up shuffle really have any difference? Do they have different periods? If so, how much do their periods differ by? The next theorem may contain the answers to these questions.

Theorem 2 *For $n \in \mathbb{N}$,n is even, let the order of $2 \quad (mod \quad (n+1))$ be $m \in \mathbb{N}$. Then in bottom-up shuffle, the period of n cards is:*
$(i)\frac{m}{2}$ if m is even and
$(-1)^{\frac{m}{2}}(2)^{\frac{m}{2}} \equiv 1 \quad (mod \quad (n+1))$ $(*)$ or
$(ii)m$, if m is even and $(*)$ does not hold true or
$(iii)2m$, if m is odd.

Proof:Let $n \in \mathbb{N}$, n is even, be the total number of cards.

Claim 1: For $x \in \mathbb{Z}$

$$f(x) = \begin{cases} n + 1 - 2x, & \text{if } x \leq \frac{n}{2} \\ 2(n+1) - 2x, & \text{if } \frac{n}{2} < x \leq n \end{cases}$$

Proof of claim: we would prove it by induction. Let there be n cards.

Base case: Since it is the bottom up shuffle, so the first card from the second stack would go to the bottom and the first card from the first stack would go to the second last position. Hence, $f(1) = (n-1)$ and $f(\frac{n}{2} + 1) = n$.

Induction hypothesis: Let for $k \in \mathbb{N}$,

$$f(k) = \begin{cases} n + 1 - 2k, & \text{if } k \leq \frac{n}{2} \\ 2(n+1) - 2k, & \text{if } \frac{n}{2} < k \leq n \end{cases}$$

Now for $(k+1)$ if both k and $k+1$ are in the same stack, then after shuffling, one card from the other stack goes between the k^{th} and $(k+1)^{th}$ card. Hence

$$f(k+1) = f(k) - 2 = \begin{cases} n+1-2(k+1), & \text{if } (k+1) \leq \frac{n}{2} \\ 2(n+1)-2(k+1), & \text{if } \frac{n}{2} < (k+1) \leq n \end{cases}$$

If k and $(k+1)$ are in different stacks then $k = \frac{n}{2}$. Then $(k+1) = \frac{n}{2}+1$. And we know $f(k+1) = f(\frac{n}{2}+1) = n$.

Hence it is true for $(k+1)$ whenever it is true for k and the base cases are already true. So

$$f(x) = \begin{cases} n+1-2x, & \text{if } x \leq \frac{n}{2} \\ 2(n+1)-2x, & \text{if } \frac{n}{2} < x \leq n \end{cases}$$

This is the end of proof of our claim.

Now notice that

$$f(x) \equiv \begin{cases} -2x, & \text{if } x \leq \frac{n}{2}, \quad (mod \quad (n+1)) \\ -2x, & \text{if } \frac{n}{2} < x \leq n \quad (mod \quad (n+1)) \end{cases}$$

Hence $f(x) \equiv -2x \quad (mod \quad n+1)$.

Claim 2: For $m \in \mathbb{N}$, $f^m(x) \equiv (-1)^m(2)^m x \quad (mod \quad (n+1))$.
Proof: Let $m \in \mathbb{N}$ .We would prove it by induction on m.
Base case: For $m=1$,

$$f^1(x) \equiv -2x \quad (mod \quad (n+1))$$
$$\implies f^1(x) \equiv (-1)^1(2)^1 x \quad (mod \quad (n+1))$$

Hence base case is true.

Induction hypothesis: let for $k \in \mathbb{N}$,

$$f^k(x) \equiv (-1)^k(2)^k x \quad (mod \quad (n+1))$$

So for $(k+1)$, $f^{k+1}(x) \equiv -2(f^k(x)) \quad (mod \quad (n+1))$

$$\implies f^{k+1}(x) \equiv -2((-1)^k(2)^k x) \quad (mod \quad (n+1))$$
$$\implies f^{k+1}(x) \equiv (-1)^{k+1}(2)^{k+1} x \quad (mod \quad (n+1))$$

So claim 2 is true for $k+1$ whenever it is true for k and the base case is true, hence it is true for all $k \in \mathbb{N}$.

This is the end of proof of claim 2.

So m is the period if $f^m(x) \equiv x \quad (mod \quad (n+1))$ for all $x \in \mathbb{N}, \quad x \leq n$.

$$\implies (-1)^m(2)^m x \equiv x \quad (mod \quad (n+1))$$

$\implies (-1)^m(2)^m \equiv 1 \quad (mod \quad (n+1))$ since x is a variable for the position of the cards.

$$(-1)^m(2)^m \equiv 1 \quad (mod \quad (n+1)) \tag{5}$$

Hence the least value of m for which (5) holds is the period of n.

Hence if α is the order of $2 \quad (mod \quad (n+1))$ then the period is :
$(i)\frac{\alpha}{2}$ if α is even and
$(-1)^{\frac{\alpha}{2}}(2)^{\frac{\alpha}{2}} \equiv 1 \quad (mod \quad (n+1))$ $\quad (*)$
$(ii)\alpha$, if α is even and $(*)$ does not hold true
$(iii)2\alpha$, if α is odd. □

4 Three Handed Shuffles

Definition 9 (Three Handed Shuffle) *We define a three-handed shuffling as the following: take a pack of m cards (where m is divisible by 3) and cut it into 3 equal parts. Call the stacks $(1),(2),(3)$ according to the order. Take the top card from each stack and and place it in a fixed order to make a new stack. Repeat the process (following a particular order of the stacks throughout the time) till there is only one stack of m cards left.*

Definition 10 (Backward Shuffle) *Define a three handed shuffle to be a backward shuffle if we take the top card of each stack in the [3-2-1] order. In other words, take the top card of the stack containing the last $\frac{m}{3}$ cards and place it. Then take the top card of the middle stack and place it on top of the existing card. Finally take the top card from the stack containing the first $\frac{m}{3}$ cards and place it on top of the new stack and continue the process till we get a new stack of m cards.*

Let us see one example: consider $n = 9$. The function f takes the following values after shuffling for the first time:
$f(1) = 7 \quad f(4) = 8 \quad f(7) = 9$
$f(2) = 4 \quad f(5) = 5 \quad f(8) = 6$
$f(3) = 1 \quad f(6) = 2 \quad f(9) = 3$
Repeating the same process gives that the period of $n = 9$ cards is 4.

Theorem 3 *For $n \in \mathbb{N}, 3|n$, let the order of $3 \pmod{(n+1)}$ be $m \in \mathbb{N}$. Then in backward three handed shuffle, the period of n cards is:*
(i)$\frac{m}{2}$ if $\frac{m}{2}$ is an odd integer and
$(-3)^{\frac{m}{2}} \equiv 1 \pmod{(n+1)}$ $\qquad (*)$ or
(ii)m, if m is even and $(*)$ does not hold $\qquad$ or
(iii)$2m$, if m is odd.

Proof: Let $n \in \mathbb{N}, 3|n$, be the total number of cards.

Claim 1: For $x \in \mathbb{Z}$

$$f(x) = \begin{cases} n+1-3x, & \text{if } x \le \frac{n}{3} \\ 2(n+1)-3x, & \text{if } \frac{n}{3} < x \le \frac{2n}{3} \\ 3(n+1)-3x, & \text{if } \frac{2n}{3} < x \le n \end{cases}$$

Proof of claim: we would prove it by induction. Let there be n cards(n is divisible by 3).

Base case: Since it is the backward shuffle, so the first card from the third stack would go to the bottom, the top card from second stack would go to second bottom position and the first card from the first stack would go to the third last position. Hence, $f(1) = (n-2)$,$f(\frac{n}{3}+1) = n-1$ and $f(\frac{2n}{3}+1) = n$.

Induction hypothesis: Let for $k \in \mathbb{N}$,

$$f(k) = \begin{cases} n+1-3k, & \text{if } k \le \frac{n}{3} \\ 2(n+1)-3k, & \text{if } \frac{n}{3} < k \le \frac{2n}{3} \\ 3(n+1)-3k, & \text{if } \frac{2n}{3} < k \le n \end{cases}$$

Notice that since there are 3 stacks, so in backward shuffle, one card from each shuffle has to be placed before taking the next card from the same stack. Now for $(k+1)$ if both k and $k+1$ are in the same stack, then after shuffling, one card from each of the three stacks goes between the k^{th} and $(k+1)^{th}$ card. Hence

$$f(k+1) = f(k) - 3 = \begin{cases} n+1-3(k+1), & \text{if } k+1 \le \frac{n}{3} \\ 2(n+1)-3(k+1), & \text{if } \frac{n}{3} < k+1 \le \frac{2n}{3} \\ 3(n+1)-3(k+1), & \text{if } \frac{2n}{3} < k+1 \le n \end{cases}$$

If k and $(k+1)$ are in different stacks then either $k = \frac{n}{3}$ or $k = \frac{2n}{3}$.So if $k = \frac{n}{3}$, then $(k+1) = \frac{n}{3}+1$. And we know $f(\frac{n}{3}+1) = n-1$. Similarly, if $f(k) = \frac{2n}{3}$ then $f(k+1) = f(\frac{2n}{3}+1) = n$.

Hence it is true for $(k+1)$ whenever it is true for k and the base cases are already true. So

$$f(x) = \begin{cases} n+1-3x, & \text{if } x \leq \frac{n}{3} \\ 2(n+1)-3x, & \text{if } \frac{n}{3} < x \leq \frac{2n}{3} \\ 3(n+1)-3x, & \text{if } \frac{2n}{3} < x \leq n \end{cases}$$

This is the end of proof of our claim.

Hence we can say that for $x \in \mathbb{N}$, $f(x) \equiv -3x \pmod{(n+1)}$.
Now if $k \in \mathbb{N}$ is the period of n cards then $\forall x, f^k(x) \equiv x \pmod{(n+1)}$.
We know $f(x) \equiv -3x \pmod{(n+1)}$.

So $f^k(x) \equiv f((f^{k-1}(x))) \pmod{(n+1)}$
$\equiv -3(f^{k-1}(x)) \pmod{(n+1)}$
$\equiv -3(-3(f^{k-2}(x))) \pmod{(n+1)}$
$\equiv (-3)^2 f^{k-2}(x) \pmod{(n+1)}$
$\equiv (-3)^k x \pmod{(n+1)}$
Hence $f^k(x) \equiv (-3)^k x \pmod{(n+1)}$

Therefore if k is the period then $f^k(x) \equiv x \pmod{(n+1)}$
$\implies (-3)^k x \equiv x \pmod{(n+1)}$
Now since x is a variable for the position of the card,
so $(-3)^k \equiv 1 \pmod{(n+1)}$.

Also we know $3|n$ so $(3, n+1) = 1$, hence if the order of 3 $\pmod{(n+1)}$ is $m \in \mathbb{N}$. Then in backward three handed shuffle, the period of n cards is:
$(i)\frac{m}{2}$ if $\frac{m}{2}$ is an odd integer and
$(-3)^{\frac{m}{2}} \equiv 1 \pmod{(n+1)}$ $(*)$ *or*
$(ii)m$, if m is even and $(*)$ does not hold or
$(iii)2m$, if m is odd. □

5 Generalised version: k Handed shuffles

At this point of time we notice that there was nothing special about the number of handed shuffles. So we try to generalise it further into k handed shuffles, where $k \in \mathbb{N}$. So we present the following theorem:

Theorem 4 *For $n, k \in \mathbb{N}, k|n$, let the order of $k \pmod{(n+1)}$ be $m \in \mathbb{N}$. Then in backward k-handed shuffle, the period of n cards is:*
$(i)\frac{m}{2}$ if $\frac{m}{2}$ is an odd integer and
$(-k)^{\frac{m}{2}} \equiv 1 \pmod{(n+1)}$ $(*)$ or
$(ii)m$, if m is even and $(*)$ does not hold or
$(iii)2m$, if m is odd.

Proof: Let $n, k \in \mathbb{N}, k|n$, and n be the total number of cards.

Claim 1: For $x \in \mathbb{Z}$

$$f(x) = \begin{cases} n+1-kx, & \text{if } x \leq \frac{n}{k} \\ 2(n+1)-kx, & \text{if } \frac{n}{k} < x \leq \frac{2n}{k} \\ 3(n+1)-kx, & \text{if } \frac{2n}{k} < x \leq \frac{3n}{k} \\ ... \\ k(n+1)-kx, & \text{if } \frac{(k-1)n}{k} < x \leq n \end{cases}$$

Proof of claim: we would prove it by induction similarly. Let there be n cards(n is divisible by k).

Base case: Since it is the backward k handed shuffle, so the top card from the last stack would be placed first, then the top card from the second last stack, and so on till the top card from the first stack is placed. Hence $f(\frac{(k-1)n}{k}+1) = n, f(\frac{(k-2)n}{k}+1) = n-1, f(\frac{(k-3)n}{k}+1) = n-3, ..., f(\frac{(2)n}{k}+1) = n-k+3, f(\frac{n}{k}+1) = n-k+2, f(1) = n-k+1,.$

Induction hypothesis: Let for $p \in \mathbb{N}$,

$$f(p) = \begin{cases} n+1-kp, & \text{if } p \leq \frac{n}{k} \\ 2(n+1)-kp, & \text{if } \frac{n}{k} < p \leq \frac{2n}{k} \\ 3(n+1)-kp, & \text{if } \frac{2n}{k} < p \leq \frac{3n}{k} \\ ... \\ k(n+1)-kp, & \text{if } \frac{(k-1)n}{k} < p \leq n \end{cases}$$

Notice that since there are k stacks, so in backward shuffle, one card from each of the stack has to be placed before taking the next card from the same stack. Now for $(p+1)$ if both p and $p+1$ are in the same stack, then after shuffling, one card from each of the k stacks goes between the p^{th} and $(p+1)^{th}$ card. Hence

$$f(p+1) = f(p) - k = \begin{cases} n+1-kp, & \text{if } p+1 \leq \frac{n}{k} \\ 2(n+1)-k(p+1), & \text{if } \frac{n}{k} < p+1 \leq \frac{2n}{k} \\ 3(n+1)-k(p+1), & \text{if } \frac{2n}{k} < p+1 \leq \frac{3n}{k} \\ ... \\ k(n+1)-k(p+1), & \text{if } \frac{(k-1)n}{k} < p+1 \leq n \end{cases}$$

Hence it is true for $(p+1)$ whenever it is true for p and the base cases are already true. So

$$f(x) = \begin{cases} n+1-kx, & \text{if } x \leq \frac{n}{k} \\ 2(n+1)-kx, & \text{if } \frac{n}{k} < x \leq \frac{2n}{k} \\ 3(n+1)-kx, & \text{if } \frac{2n}{k} < x \leq \frac{3n}{k} \\ ... \\ k(n+1)-kx, & \text{if } \frac{(k-1)n}{k} < x \leq n \end{cases}$$

This is the end of proof of our claim.

Hence we can say that for $x \in \mathbb{N}$, $f(x) \equiv -kx \pmod{(n+1)}$.

Claim 2 : For $a \in \mathbb{N}, f^a(x) \equiv (-k)^a x \pmod{(n+1)}$.

Proof by induction:

Base case: For $a = 1, f(x) \equiv (-k)x$, which we derived earlier. Hence base case is true.

Induction Hypothesis: Let for $p \in \mathbb{N}, f^p(x) \equiv (-k)^p x \pmod{(n+1)}$.

So for $p+1$, $f^{p+1}(x) \equiv f(f^p(x)) \pmod{(n+1)}$
$\implies f^{p+1}(x) \equiv f((-k)^p x) \pmod{(n+1)}$
$\equiv (-k)((-k)^p x) \pmod{(n+1)}$
$\equiv (-k)^{p+1} x \pmod{(n+1)}$
$\implies f^{p+1}(x) \equiv (-k)^{p+1} x \pmod{(n+1)}$ Hence it is true for $p+1$ whenever it is true for p, and it is already true for base cases, so by induction it is true for all $k \in \mathbb{N}$.

this is the end of claim 2.

Now if $a \in \mathbb{N}$ is the period of n cards then $\forall x, f^a(x) \equiv x \pmod{(n+1)}$.

Therefore if a is the period then $f^a(x) \equiv x \pmod{(n+1)}$
$\implies (-k)^a x \equiv x \pmod{(n+1)}$

Now since x is a variable for the position of the card,
so $(-k)^a \equiv 1 \pmod{(n+1)}$.

Also we know $k|n$ so $(k, n+1) = 1$, hence if the order of $k \pmod{(n+1)}$ is $m \in \mathbb{N}$. Then in backward k handed shuffle, the period of n cards is:
$(i)\frac{m}{2}$ if $\frac{m}{2}$ is an odd integer and
$(-k)^{\frac{m}{2}} \equiv 1 \pmod{(n+1)}$ $\quad (*) \quad$ *or*
$(ii)m$, if m is even and $(*)$ does not hold or
$(iii)2m$, if m is odd. □

6 Appendix

Definition 11 *Given $n \in \mathbb{Z}$, n is called even if $n \equiv 0 \pmod 2$.*

Definition 12 *Given $n \in \mathbb{Z}$, n is called odd if $n \equiv 1 \pmod 2$.*

Definition 13 (Trichotomy) *If $n \in \mathbb{Z}$, the exactly one of the following is true:*
(1)$n \in \mathbb{N}$
(2)$n = 0$
(3)$(-n) \in \mathbb{N}$.

Definition 14 (Trichotomy of Ordering) *If $a, b \in \mathbb{Z}$, the exactly one of the following is true:*
(1)$a > b$
(2)$a = b$
(3)$a < b$.

Figure 1: Table of Periods

No. of Cards	TU Period	BU Period	TD Period	BD Period
2	2	1	2	1
4	2	4	4	2
6	4	6	3	4
8	6	3	6	3
10	6	5	10	6
12	10	12	12	10

Figure 2-: Tables of ...

4TU	4BU	4TD	4BD
1,2,3,4	1,2,3,4	1,2,3,4	1,2,3,4
4,2,3,1	2,4,1,3	3,1,4,2	1,3,2,4
1,2,3,4	4,3,2,1	4,3,2,1	1,2,3,4
-	3,1,4,2	2,4,1,3	-
-	1,2,3,4	1,2,3,4	-

6TU	6BU	6TD	6BD
1,2,3,4,5,6	1,2,3,4,5,6	1,2,3,4,5,6	1,2,3,4,5,6
6,3,5,2,4,1	3,6,2,5,1,4	4,1,5,2,6,3	1,4,2,5,3,6
1,5,4,3,2,6	2,4,6,1,3,5	2,4,6,1,3,5	1,5,4,3,2,6
6,4,2,5,3,1	6,5,4,3,2,1	1,2,3,4,5,6	1,3,5,2,4,6
1,2,3,4,5,6	4,1,5,2,6,3	-	1,2,3,4,5,6
-	5,3,1,6,4,2	-	-
-	1,2,3,4,5,6	-	-

8TU	8BU	8TD	8BD
1,2,3,4,5,6,7,8	1,2,3,4,5,6,7,8	1,2,3,4,5,6,7,8	1,2,3,4,5,6,7,8
8,4,7,3,6,2,5,1	4,8,3,7,2,6,1,5	5,1,6,2,7,3,8,4	1,5,2,6,3,7,4,8
1,3,5,7,2,4,6,8	7,5,3,1,8,6,4,2	7,5,3,1,8,6,4,2	1,3,5,7,2,4,6,8
8,7,6,5,4,3,2,1	1,2,3,4,5,6,7,8	8,7,6,5,4,3,2,1	1,2,3,4,5,6,7,8
1,5,2,6,3,7,4,8	-	4,8,3,7,2,6,1,5	-
8,6,4,2,7,5,3,1	-	2,4,6,8,1,3,5,7	-
1,2,3,4,5,6,7,8	-	1,2,3,4,5,6,7,8	-

10TU	10BU	10TD	10BD
1,2,3,4,5,6,7,8,9,10	1,2,3,4,5,6,7,8,9,10	1,2,3,4,5,6,7,8,9,10	1,2,3,4,5,6,7,8,9,10
10,9,5,4,8,3,7,2,6,1	5,10,4,9,3,8,2,7,1,6	6,1,7,2,8,3,9,4,10,5	1,6,2,7,3,8,4,9,5,10
1,8,6,4,2,9,7,5,3,10	3,6,9,1,4,7,10,2,5,8	3,6,9,1,4,7,10,2,5,8	1,8,6,4,2,9,7,5,3,10
10,2,3,4,5,6,7,8,9,1	4,8,5,1,9,2,6,10,3,7	7,3,10,6,2,9,5,1,8,4	1,9,8,7,6,5,4,3,2,10
1,5,9,4,8,3,7,2,6,10	9,7,5,3,1,10,8,6,4,2	9,7,5,3,1,10,8,6,4,2	1,5,9,4,8,3,7,2,6,10
10,8,6,4,2,9,7,5,3,1	1,2,3,4,5,6,7,8,9,10	10,9,8,7,6,5,4,3,2,1	1,3,5,7,9,2,4,6,8,10
1,2,3,4,5,6,7,8,9,10	-	5,10,4,9,3,8,2,7,1,6	1,2,3,4,5,6,7,8,9,10
-	-	8,5,2,10,7,4,1,9,6,3	-
-	-	4,8,9,5,1,2,6,10,3,7	-
-	-	2,4,6,8,10,1,3,5,7,9	-
-	-	1,2,3,4,5,6,7,8,9,10	-

12TU	12BU	12TD	12BD
1,2,3,4,5,6,7,8,9,10,11,12	1,2,3,4,5,6,7,8,9,10,11,12	1,2,3,4,5,6,7,8,9,10,11,12	1,2,3,4,5,6,7,8,9,10,11,12
12,6,11,5,10,4,9,3,8,2,7,1	6,12,5,11,4,10,3,9,2,8,1,7	7, 1,8,2,9,3,10,4,11,5,12,6	1,7,2,8,3,9,4,10,5,11,6,12
1,4,7,10,2,5,8,11,3,6,9,12	10,7,4,1,11,8,5,2,12,9,6,3	10, 7,4,1,11,8,5,2,12,9,6,3	1,4,7,10,2,5,8,11,3,6,9,12
12,5,9,2,6,10,3,7,11,4,8,1	8,3,11,6,1,9,4,12,7,2,10,5	5,10,2,7,12,4,9,1,6,11,3,8	1,8,4,11,7,3,10,6,2,9,5,12
1,10,8,6,4,2,11,9,7,5,3,12	9,5,1,10,6,2,11,7,3,12,8,4	9,5,1,10,6,2,11,7,3,12,8,4	1,10,8,6,4,2,11,9,7,5,3,12
12,2,3,4,5,6,7,8,9,10,11,1	2,4,6,8,10,12,1,3,5,7,9,11	11, 9,7,5,3,1,12,10,8,6,4,2	1,11,10,9,8,7,6,5,4,3,2,12
1,6,11,5,10,4,9,3,8,2,7,12	12,11,10,9,8,7,6,5,4,3,2,1	12,11,10,9,8,7,6,5,4,3,2,1	1,6,11,5,10,4,9,3,8,2,7,12
12,4,7,10,2,5,8,11,3,6,9,1	7,1,8,2,9,3,10,4,11,5,12,6	6,12,5,11,4,10,3,9,2,8,1,7	1,9,6,3,11,8,5,2,10,7,4,12
1,5,9,2,6,10,3,7,11,4,8,12	3,6,9,12,2,5,8,11,1,4,7,10	3,6,9,12,2,5,8,11,1,4,7,10	1,5,9,2,6,10,3,7,11,4,8,12
12,10,8,6,4,2,11,9,7,5,3,1	5,10,2,7,12,4,9,1,6,11,3,8	8, 3,11,6,1,9,4,12,7,2,10,5	1,3,5,7,9,11,2,4,6,8,10,12
1,2,3,4,5,6,7,8,9,10,11,12	4,8,12,3,7,11,2,6,10,1,5,9	4,8,12,3,7,11,2,6,10,1,5,9	1,2,3,4,5,6,7,8,9,10,11,12
-	11,9,7,5,3,1,12,10,8,6,4,2	8,2,4,6,8,10,12,1,3,5,7,9,11	-
-	1,2,3,4,5,6,7,8,9,10,11,12	1,2,3,4,5,6,7,8,9,10,11,12	-