Shuffling Your Way Around (Odd Card Out)

The problem here is to find out the number of shuffles needed for all the cards in a deck of n cards, where n is odd, to be stacked in the original order.

We number the cards in the deck of n cards as follows: the card at the top of the deck is in position 1, the card directly below is in position 2, and so on (the card at the bottom of the deck is in position n).

Let $m = \frac{n-1}{2}$. During a shuffle, a deck is split into two (decks A and B), with one consisting of m cards and the other $m+1$ cards. After the cards are shuffled, all cards with odd-numbered positions are from deck A and cards with even-numbered positions are from deck B, or vice versa. The former is called an out shuffle while the latter is called an in shuffle. The deck can be split in two ways:

1. Deck A has m cards, containing cards in position $1, 2,$ ... m, while Deck B has $m+1$ cards, containing cards in position $m+1, m+2,$ ... n

2. Deck A has $m+1$ cards, containing cards in position $1, 2,$ ... $m+1$, while Deck B has m cards, containing cards in position $m+2, m+3,$ ... n

So the deck can be shuffled in 4 ways:

1. Deck A has m cards and Deck B has $m+1$ cards, each shuffle is an out shuffle

2. Deck A has m cards and Deck B has $m+1$ cards, each shuffle is an in shuffle

3. Deck A has $m+1$ cards and Deck B has m cards, each shuffle is an out shuffle

4. Deck A has $m+1$ cards and Deck B has m cards, each shuffle is an in shuffle

For each case, the cards are stacked in the following order after a shuffle:

Card Position

	After Shuffle			
Before Shuffle	Case 1	Case 2	Case 3	Case 4
1	1	2	1	2
2	3	4	3	4
3	5	6	5	6
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$m-1$	$n-4$	$n-3$	$n-4$	$n-3$
m	$n-2$	$n-1$	$n-2$	$n-1$
$m+1$	2	1	n	n
$m+2$	4	3	2	1
$m+3$	6	5	4	3
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$n-1$	$n-1$	$n-2$	$n-3$	$n-4$
n	n	n	$n-1$	$n-2$

For $1 \leq i < b$, where b is a positive integer, let $C_i(b) = \{2^j \cdot i \ (mod\ b) \mid j \geq 1\}$.

Let $k = |C_1(b)|$. So $C_1(b) = \{1, 2, 2^2, \ldots 2^{k-1}\}$. Since $2^{\phi}(b) = 1\ (mod\ b)$, k is a factor of $\phi(b)$, where $\phi(b)$ is the number of integers between 1 and b which are coprime with b, for any b. (If $b = \Pi_{i=1}^{m}\ p_i^{a_i}$ is the prime factorization of n, $\phi(b) = \Pi_{i=1}^{m}\ p_i^{(a_i-1)}$.)

If a deck contain n cards, where n is even, the deck would be stacked in the original order after $C_1(n+1)$ and $C_1(n-1)$ in and out shuffles respectively.

Notice the following:

1. For Case 1, the card at the bottom (position n) of the deck remains at the bottom after a shuffle. So, by removing card n from the deck, case 1 is equivalent to an out shuffle of $n-1$ cards. Thus $C_1(n-2)$ shuffles is needed.

2. For Case 2, the card at the bottom (position n) of the deck remains at the bottom after a shuffle. So, by removing card n from the deck, case 2 is equivalent to an in shuffle of $n-1$ cards. Thus $C_1(n)$ shuffles is needed.

3. For Case 3, the card at the top (position 1) of the deck remains at the top after a shuffle after a shuffle. So, by removing card 1 from the deck, case 3 is equivalent to an in shuffle of $n-1$ cards. Thus $C_1(n)$ shuffles is needed.

For Case 4, the card position of all cards changes after a shuffle. So this case has to be considered separately.

Since $m = \frac{n-1}{2}$, $2m = n-1$. Also note that

$$2(m+2) = n - 1 + 2 \cdot 2 = n + 3 = 1(mod\ n+2)$$

$$2(m+3) = n - 1 + 2 \cdot 3 = n + 5 = 3(mod\ n+2)$$

$$\vdots$$
$$2n = (n+2) + (n-2) = n - 2(mod\ n+2)$$

However, $2(m+1) = n-1+2\cdot 1 = n+1(mod\ n+2)$. So we cannot express Case 4 with the function:

$$f(i) = 2i(mod\ n+2),\ \ i = 1, 2, \ldots, n$$

Now suppose we add an (imaginary) card $n+1 = 2m+2$ to the deck. The card order after an in shuffle would be as follows:

Card Position	
Before Shuffle	After Shuffle
1	2
2	4
$\vdots$	$\vdots$
$m-1$	$n-3$
m	$n-1$
$m+1$	$n+1$
$m+2$	1
$\vdots$	$\vdots$
n	$n-2$
$n+1$	n

This is an in shuffle of $n+1$ cards, so it can be expressed by the function

$$f(i) = 2i(mod\ n+2),\ \ i = 1, 2, \ldots n+1$$

.

Notice that $2(m+1) = n+1(mod\ n+2)$ and $2(n+1) = n(mod\ n+2)$. So $4(m+1) = 2\cdot 2(m+1) = n(mod\ n+2)$.

By definition of $C_i(b)$, we can obtain elements of $C_j(n+2)$, where $1 \le j \le n+2$, by multiplying elements of $C_1(n+2)$ by j. Since $2^k = 1\ (mod\ n+2)$, $2^k j = j\ (mod\ n+2)$. So, for any $1 \le j \le n$, $|C_j(n+2)|$ is either k or a factor of k.

We now show that $|C_n(n+2)| = |C_1(n+2)|$. Suppose $2^s \cdot n = 2^t \cdot n(mod\ n+2), 0 \le s < t < k$. Since n is odd, n and $n+2$ are coprime (otherwise 2 would be a common factor of n and $n+2$, a contradiction).

So we can divide both sides of $2^s \cdot n = 2^t \cdot n\ (mod\ n+2)$ by n to obtain

$$2^s = 2^t\ (mod\ n+2)$$

Since n is odd, $n+2$ is odd. Thus 2 and $n+2$ are coprime. So 2^a is coprime with $n+2$ for any $a \ge 1$.

So we can divide both sides $2^s = 2^t\ (mod\ n+2)$ by 2^s to obtain

$$1 = 2^{t-s}\ (mod\ n+2)$$

Thus $|C_1(n+2)| = t-s < k$, a contradiction. So $|C_n(n+2)| = |C_1(n+2)| = k$.

Now $2(n+1) = n\ (mod\ n+2)$ and $2^k n = n\ (mod\ n+2)$. Since n is odd, $n+2$ is odd and thus 2 and $n+2$ are coprime. So we have

$$2(n+1) = 2^k n\ (mod\ n+2)$$

$$n+1 = 2^{k-1} n\ (mod\ n+2)$$

Thus $n+1 \in C_n(n+2)$. However, card $n+1$ is not in the deck. So we need to remove $n+1$ from the set $C_n(n+2)$. Thus all cards in $C_n(n+2)$ would return to their original position after $|C_n(n+2)|' = k-1$ shuffles.

Now, all cards in $C_1(n+2)$ return to their original positions after $k = |C_1(n+2|$ shuffles. Likewise, for any $1 \leq j \leq n-1$, all cards in $C_j(n+2)|$ return to their original positions after $|C_j(n+2)|$ shuffles.

So the deck would be stacked in the original order after $LCM\,(|C_1(n+2)|,\ |C_2(n+2))|,\ \ldots |C_{n-1}(n+2)|, |C_n(n+2)|')$ shuffles.

For all j where $1 \leq j \leq n-1$, $|C_j(n+2)|$ is a factor of $|C_1(n+2)|$. So

$$LCM\,(|C_1(n+2)|,\ |C_2(n+2))|,\ \ldots |C_{n-1}(n+2)|) = k$$

Thus, for Case 4, the deck would be stacked in the original order after the following number of shuffles:

$$\begin{aligned} & LCM\,(|C_1(n+2)|,\ |C_2(n+2))|,\ \ldots |C_{n-1}(n+2)|, |C_n(n+2)|') \\ & = LCM\,(LCM\,[|C_1(n+2)|,\ |C_2(n+2))|,\ \ldots |C_{n-1}(n+2)|]\,, |C(n)|') \\ & = LCM\,(k, k-1) \end{aligned}$$

So suppose we have a regular set of playing cards (including the Joker). Here we have a deck of $n = 53$ cards. So $n-2 = 51$ and $n+2 = 55$. We know that $|C_1(51)| = 8$ and $|C_1(53)| = 52$.

Now $\phi(55) = \phi(11 \cdot 5) = \phi(11)\phi(5) = 10 \cdot 4 = 40$. The factors of 40 are 1, 2, 4, 5, 8, 10, 20 and 40. So we have the following:

i	$2^i\ (mod\ 55)$
1	2
2	4
4	16
5	32
8	36
10	34
20	1

So $C_1(55)| = 20$. Thus the deck of $n = 53$ cards would be stacked in the original order after the following number of shuffles:

Case	Number of Shuffles
1	8
2	52
3	52
4	LCM (20, 20-1) = 380

Note that if we perform Case 4 shuffles, the number of schuffles needed for the deck to be stacked in its original order may be smaller, but it is always a factor of $LCM\,(k, k-1)$.