Shuffling Your Way Around

In card games, the deck is shuffled between games so that the cards will not be dealt in the same order. However, if one shuffles perfectly the cards will eventually stacked in the original order. The question is how many shuffles are required for that to happen.

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).

During a shuffle, a deck is split into two (decks A and B), each consists of exactly half the deck. So deck A consists of cards with positions 1 to $\frac{n}{2}$ and deck B consists of cards in positions $\frac{n}{2} + 1$ to n.

We define a perfect shuffle as follows: 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.

If n is even and we do an in shuffle, the cards before and after the shuffle would be in the following order:

Card Position	
Before Shuffle	After Shuffle
1	2
2	4
3	6
$\vdots$	$\vdots$
$\frac{n}{2}$	n
$\frac{n}{2}+1$	1
$\frac{n}{2}+2$	3
$\vdots$	$\vdots$
n	$n-1$

Notice the following

$$2\left(\frac{n}{2}+1\right) = n+2 = 1 \ (mod\ n+1)$$

$$2\left(\frac{n}{2}+2\right) = n+4 = 3 \ (mod\ n+1)$$

$$2n = n-1 \ (mod\ n+1)$$

So if a card is in position i before the shuffle, the card is in position $2i\ (mod\ n+1)$ after the shuffle.

So the in shuffle can be expressed as the following function:

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

Since n is even, $n+1$ is odd and thus coprime with 2.

Let m be the number of in shuffles needed before the cards return to the original position. So we are trying to find m such that $2^m = 1\ (mod\ n+1)$.

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 $k = |C_1(n+1)|$. So $C_1(n+1) = \{1, 2, 2^2, \ldots 2^{k-1}\}$. By definition of $C_i(n+1)$, we can obtain elements of $C_j(n+1)$, where $1 \leq j \leq n$, by multiplying elements of $C_1(n+1)$ by j. Since $2^k = 1\ (mod\ b)$, $2^k j = j\ (mod\ n+1)$. So, for any $1 \leq j \leq n$, $|C_j(b)|$ is either k or a factor of k. So the deck would be stacked in the original order after k in shuffles.

Now let $\phi(n)$ be the number of integers between 1 and n which are coprime with n. (For example, if $n = 6$, we see that 1 and 5 are coprime with n. So $\phi(n) = 2$.)

If $n = p_1^{a_1} p_2^{a_2} \ldots p_s^{a_s}$, where $p_1, p_2, \ldots p_s$ are distinct primes, then

$$\phi(n) = \prod_{i=1}^{s} \left(p_i^{a_i} - p_i^{(a_i - 1)} \right)$$

We now show how $\phi(n)$ is computed . First suppose p is prime. The only factors of p are 1 and itself. So each of $1, 2, \ldots p-1$ are coprime with p. Thus $\phi(p) = p - 1$.

Now we consider $\phi(p^a)$ for $a > 1$. Since p is prime, any integer between 1 and p^a which is not a multiple of p is coprime with p. Since there are $p^a/p = p^{a-1}$ integers between 1 and p^a which are multiples of p, $\phi(p^a) = p^a - p^{a-1}$.

Now we consider the value of $\phi(n)$, where $n = pq$ and p, q are distinct primes. The factors of pq are $1, p, q$ and pq. So any integer $i, 1 \leq i \leq pq$ is coprime with pq if it is not a multiple of p or q. Let P and Q be the set of multiples of p and q between 1 and n respectively. Now there are q integers $(p, 2p, \ldots pq)$ in the set P. Likewise, there are p integers $(q, 2q, \ldots pq)$ in the set Q.

Since p, q are prime, pq is the only integer contained in both P and Q. Since the two sets have one common integer, there are $p + q - 1$ integers between 1 and pq which are multiples of either p or q.

So there are $pq - (p+q-1) = pq - p - q + 1 = (p-1)(q-1)$ integers between 1 and pq which are coprime with pq. Thus $\phi(pq) = \phi(p)\phi(q)$.

We now consider $n = p^a q^b$, where p, q are distinct primes and $a, b \geq 1$. Since p, q are prime, a number between 1 and n is coprime with n if it is not a multiple of either p or q. Let P and Q be the set of multiples of p and q between 1 and n respectively. So there are $n/p = p^{a-1}q^b$ integers in the set P and $n/q = p^a q^{b-1}$ integers in the set Q.

Let PQ be the set of integers between 1 and n which are multiples of both p or q, or multiples of pq. So there are $n/pq = p^{a-1}q^{b-1}$ integers in the set PQ. The latter has to be subtracted from the total number of multiples of either p or q as integers in the set PQ are contained in both P and Q.

So there are $p^{a-1}q^b + p^a q^{b-1} - p^{a-1}q^{b-1}$ integers between 1 and $p^a q^b$ which are multiples of either p or q. Thus $\phi(n)$, the number of integers between 1 and

n which are coprime with n, is

$$\begin{aligned}p^aq^b-(p^{a-1}q^b+p^aq^{b-1}-p^{a-1}q^{b-1}) &= p^aq^b-p^{a-1}q^b-p^aq^{b-1}+p^{a-1}q^{b-1}\\ &= p^aq^b-p^aq^{b-1}-p^{a-1}q^b+p^{a-1}q^{b-1}\\ &= p^a(q^b-q^{b-1})-p^{a-1}(q^b-q^{b-1})\\ &= (p^a-p^{a-1})(q^b-q^{b-1})\\ &= \phi(p^a)\phi(q^b)\end{aligned}$$

Now consider $n=p^aq^br^c$, where p,q,r are distinct primes and $a,b,c\geq 1$. Since p,q,r are prime, a number between 1 and n is coprime with n if it is not a multiple of either p, q or r. Let P,Q,R be the set of multiples of p,q and r between 1 and n respectively and $|P|,|Q|$ and $|R|$ be the number of integers in the sets P,Q and R respectively. So we have $|P|=n/p=p^{a-1}q^br^c$, $|Q|=n/q=p^aq^{b-1}r^c$ and $|R|=n/r=p^aq^br^{c-1}$.

Let PQ,PR and QR be set of integers between 1 and n which are multiples of pq, pr and qr respectively and $|PQ|,|PR|$ and $|QR|$ be the number of integers in the sets PQ,PR and QR respectively. Now $|PQ|=n/pq=p^{a-1}q^{b-1}r^c$, $|PR|=n/pr=p^{a-1}q^br^{c-1}$ and $|QR|=n/qr=p^aq^{b-1}r^{c-1}$. Let PQR be set of integers between 1 and n which are multiples of pqr. Now there are $|PRQ|=n/pqr=p^{a-1}q^{b-1}r^{c-1}$ integers in the set PQR.

As shown above, $|PQ|,|PR|,|QR|$ have to be subtracted from the total number of integers between 1 and n which are multiples of either p,q or r. However, this would exclude multiples of pqr from the set of integers between 1 and n which are multiples of either p,q or r. So the number of integers between 1 and n which are multiples of either p,q or r is $|P|+|Q|+|R|-|PQ|-|PR|-|QR|+|PQR|$ and $\phi(n)=n-(|P|+|Q|+|R|-|PQ|-|PR|-|QR|+|PQR|)$.

Thus $\phi(n)$ is

$$\begin{aligned}&p^aq^br^c-p^{a-1}q^br^c-p^aq^{b-1}r^c-p^aq^br^{c-1}+p^{a-1}q^{b-1}r^c+p^{a-1}q^br^{c-1}+p^aq^{b-1}r^{c-1}-p^{a-1}q^{b-1}r^{c-1}\\ &=p^{a-1}q^{b-1}r^{c-1}(pqr-qr-pr-pq+r+q+p-1)\\ &=p^{a-1}q^{b-1}r^{c-1}(p-1)(q-1)(r-1)\\ &=p^{a-1}(p-1)q^{b-1}(q-1)r^{c-1}(r-1)\\ &=(p^a-p^{a-1})(q^b-q^{b-1})(r^c-r^{c-1})\\ &=\phi(p^a)\phi(q^b)\phi(r^c)\end{aligned}$$

By applying similar arguement repeatedly, we will find that if $n=p_1^{a_1}p_2^{a_2}...p_s^{a_s}$, where $p_1,p_2,...p_s$ are distinct primes,

$$\phi(n)=\prod_{i=1}^{s}\left(p_i^{a_i}-p_i^{(a_i-1)}\right)$$

Let $P(n)$ be the set of integers between 1 and n which are coprime with n. So $|P(n)|=\phi(n)$. We denote the integers in the set $P(n)$ as $a_1,a_2,...a_{\phi(n)}$. For each $a_i, 1\leq a_i<n$.

Now for all $i, j, k \in P(n)$, $ij \neq ik (mod\ n)$. To show this, suppose $ij = ik(mod\ n)$ for some $i, j, k \in P(n)$. So we have

$$ij = ik\ (mod\ n)$$
$$i(j-k) = 0\ (mod\ n)$$

Since $i \in P(n)$, i and n have no common prime factors. So we can divide both sides of the above equation by i. Thus $j-k = 0\ (mod\, n)$. Since $j, k \in P(n)$, $1 \leq j < n$ and $1 \leq k < n$. So $j-k = 0$. Now 2 is coprime with any odd number. Thus for any odd number n, $\{a_1, a_2, ...a_{\phi(n)}\} = \{2a_1, 2a_2, ...2a_{\phi(n)}\}$.

So for any odd number n, we have

$$\begin{aligned} a_1a_2...a_{\phi(n)} &= (2a_1)(2a_2)...(2a_{\phi(n)})\ (mod\ n) \\ &= 2^{\phi(n)}a_1a_2...a_{\phi(n)}\ (mod\ n) \end{aligned}$$

Since each a_i is coprime with n, we can divide both sides of the above equation by $a_1a_2...a_{\phi(n)}$ to obtain the following:

$$1 = 2^{\phi(n)}\ (mod\ n)$$

Since $k = |C_1(n+1)|$, by the definition of $C_1(n+1)$, $2^k = 1\ (mod\ n+1)$ and $2^i \neq 1\ (mod\ n+1)$ for any $1 \leq i < k$. Now $1^j = 1\ (mod\ n+1)$ for any non-negative integer j. Thus k is a factor of $\phi(n+1)$.

Suppose we have a deck of regular playing cards ($n = 52$). Now $\phi(52+1) = \phi(53) = 52$. The factors of 52 are 1, 2, 4, 13, 26 and 52, so we have the following:

i	$2^i\ (mod\ 53)$
1	2
2	4
4	16
13	30
26	52
52	1

Thus $k = 52$ and the deck would be stacked in the original order after 52 in shuffles.

Now suppose n is even and we do an out shuffle, the cards before and after the shuffle would be in the following order:

Card Position	
Before Shuffle	After Shuffle
1	1
2	3
3	5
$\vdots$	$\vdots$
$\frac{n}{2}$	$n-1$
$\frac{n}{2}+1$	2
$\frac{n}{2}+2$	4
$\vdots$	$\vdots$
$n-1$	$n-2$
n	n

Notice that cards 1 and n remain in their original position after an out shuffle. So if we remove cards 1 and n from the deck, we have a deck with $n-2$ cards (card 2 becomes card 1 in the new deck, card 3 becomes card 2 and so forth, with card $n-1$ becoming card $n-2$) and the cards in the new deck would be in the following order after a shuffle:

Card Position	
Before Shuffle	After Shuffle
1	2
2	4
$\vdots$	$\vdots$
$\frac{n}{2}-1$	$n-2$
$\frac{n}{2}$	1
$\frac{n}{2}+1$	3
$\vdots$	$\vdots$
$n-2$	$n-3$

Notice that the above is an out shuffle for a deck with $n-2$ cards.

By the above reasoning, the cards would be stacked in the original order after $m = \phi(n-2+1) = \phi(n-1)$ out shuffles.

Suppose we have a regular set of playing cards ($n = 52$). We have $\phi(52-1) = \phi(51) = \phi(17) \cdot \phi(3) = 16 \cdot 2 = 32$. Now the factors of 32 are 1, 2, 4, 8, 16 and 32. So we have the following:

i	2^i $(mod\ 51)$
1	2
2	4
4	16
8	1

So $k = 8$ and the deck would be stacked in the original order after 8 out shuffles.