Perfect Shuffles

Number the locations in a deck by how many cards are above them:

0 1 2 3 4 5 ... n

In one perfect shuffle a card at location \( x \) in a deck of \( n \) cards is moved to location \( 2x \mod n \).

It is fairly easy to convince yourself of this. Cards in the top half of the deck are easy. If \( x \) cards are above them, \( x \) more are inserted above them when we do a shuffle.

So if we do \( k \) shuffles cards starting at location \( x \) end

at location \( 2^k x \mod n \).

If \( 2^m - 1 \mod n \) then \( m \) perfect shuffles returns a deck of \( n \) cards to their original arrangement.

It can happen that there is an exponent on \( x \) like numbers \( x \) and \( y \) so that \( 2^x \equiv x, 2^y \equiv y \mod n \),

but \( 2^m \equiv 1 \mod n \).

Still, we can answer the "how many shuffles to \( n \) cards" question by finding the smallest positive number \( m \) so that \( 2^m \equiv 1 \mod n \).

Example: repeated doubling modulo 51

1, 2, 4, 8, 16, 32, 64 \equiv 13, 26, 52 \equiv 1

shows \( 2^5 \equiv 1 \mod 51 \), so

a perfect deck of a standard deck returns it to its original order.