GEORGE ANDREW’S RIFFLE PROBLEM

The problem appears as Exercise 2 on page 57 of George Andrew’s book *Number Theory* (Dover 1994). The problem refers to a deck of $2^n$ cards. We shall illustrate the problem and two solutions by using $n = 3$. It should be clear afterwards that the solutions work for any value of $n$. We shall label the cards in bold face as $0, 1, 2, 3, 4, 5, 6, 7$.

After the riffle the cards appear in the order $0, 7, 1, 6, 2, 5, 3, 4$.

So the riffle corresponds to the permutation $\pi$ given by

$$\pi(0) = 0, \pi(1) = 2, \pi(2) = 4, \pi(3) = 6, \pi(4) = 7, \pi(5) = 5, \pi(6) = 3, \pi(7) = 1.$$  

We have to prove that

$$\pi^{(4)}(j) = (\pi \circ \pi \circ \pi \circ \pi)(j) \quad j = 0, 1, 2, \ldots, 7.$$  

In other words, after four such riffles, the deck of cards returns to its original order.

**SOLUTION USING $\mathbb{Z}_{15}$.**

We get a well-defined function on $\mathbb{Z}_{15}$ by the formula $\phi(j) = 2j$. We relate the seven cards to the numbers in $\mathbb{Z}_{15}$ as in the diagram below:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14

0, 1, 2, 3, 4, 5, 6, 7, 7, 6, 5, 4, 3, 2, 1

Notice that the cards opposite numbers $t_1$ and $t_2$ are identical if and only if $t_1 + t_2 = 15$. Since $2t_1 + 2t_2 = 30$, it follows that the cards opposite $2t_1$ and $2t_2$ are equally identical. It is now easy to check that the function $\phi(t) = 2t$ on $\mathbb{Z}_{15}$ corresponds precisely to the permutation $\pi$ above. But

$$\phi^{(4)}(t) = (\phi \circ \phi \circ \phi \circ \phi)(t) = 2^4 t \equiv t \pmod{15}.$$  

The proof is complete!
SOLUTION USING BINARY ARITHMETIC

Now we represent the cards in binary arithmetic as:

000, 001, 010, 011, 100, 101, 110, 111

We shall use Greek letters to denote “words” in 0 and 1; for example, $\alpha = 01$. Given a word $\alpha$ we write $\alpha^*$ for the word in which every 0 in $\alpha$ is replaced by a 1, and every 1 in $\alpha$ is replaced by a 0. Notice that $\alpha + \alpha^*$ is the word consisting of all 1’s. We reinterpret the permutation $\pi$ above in terms of words. For $x = 0, 1, 2, 3$ we have $\pi(x) = 2x$ and so

$$\pi(0\alpha) = \alpha0.$$  

For $x = 4 + t$ with $t = 0, 1, 2, 3$, we have $\pi(x) = 8 - (2t + 1)$ and so

$$\pi(1\alpha) = 1000 - \alpha0 - 001 = \alpha^1.$$  

You should now convince yourself that these formulas for $\pi$ work in the general case for $2^n$ cards; from now on we shall suppose we are in the general case. The length of the word $\alpha$ is the number of letters in the word, and is denoted by $|\alpha|$. Thus $|011010| = 6$. Start calculating $\pi(2), \pi(3), \ldots$ for lots of words and you will soon conjecture the following Lemma (which we can prove by induction much more quickly than it took to guess the formulas!).

**Lemma.** For $n = |\alpha| + 1$, and for any word $\beta$ (including the empty word) we have

$$\pi^{(n)}(\alpha0\beta) = \beta0\alpha, \quad \pi^{(n)}(\alpha1\beta) = \beta^*1\alpha^*.$$  

**Proof.** We use induction on $n$. When $n = 1$, the word $\alpha$ is empty and the required equations are just the above equations for $\pi$. Suppose the result holds for $n$. Increase the length of $\alpha$ by one letter and we have to consider what happens for the four possible cases:

$$\alpha00\beta, \quad \alpha10\beta, \quad \alpha01\beta, \quad \alpha11\beta.$$  

We have

$$\pi^{(n+1)}((\alpha0)0\beta) = \pi(\pi^{(n)}(\alpha0(0\beta))) = \pi((0\beta)0\alpha) = \beta0(\alpha0)$$

$$\pi^{(n+1)}((\alpha1)0\beta) = \pi(\pi^{(n)}(\alpha1(0\beta))) = \pi((0\beta)^*1\alpha^*) = \pi(1(\beta^*1\alpha^*)) = \beta0(\alpha1).$$
We leave you to check the other two cases. The result follows by the principle of Induction.

Notice that the argument does NOT exclude the case in which $\beta$ is the empty word. So we have proved in particular that $\pi(n)(\alpha_0) = 0\alpha$ and $\pi(n)(\alpha_1) = 1\alpha^*$. Apply the permutation $\pi$ once more and we see that the deck of cards does indeed return to its original order in $n + 1$ steps. There is a subtle point in the above argument. Why did we not go the whole hog and prove directly by induction on $|\alpha|$ that

$$\pi^{(n+1)}(\alpha_0) = \alpha_0, \quad \pi^{(n+1)}(\alpha_1) = \alpha_1$$

It is because if we mimic the above proof we need to know that the lemma holds not only for the empty word $\beta$ but also when $\beta$ has length 1. To prove the latter case bare hands we need to know that the lemma holds also when $\beta$ has length 2. We keep chasing our tail and never catch it! We got round this by making the inductive statement apply to an arbitrary word $\beta$.

P.S. If you are into permutations you may like to tackle the (non-trivial) problem of breaking $\pi$ down into its component disjoint cycles.