Solution to Problem F3

based on solution by Neil Spalter

F1. Look for a pattern in the remainders of the derangement numbers D_n, modulo m. (The *modulus* m is the divisor that gives the remainder.) Both the pattern itself and its length are worth thinking about.

F3. Prove that in F1 there is always a finite repeating pattern, no matter what positive integer m is.

We're looking for a *period* of $D_n \bmod m$. A period p is a positive integer such that $D_n = D_{n+p}$ for every $n \geq 0$. (Ideally, we'd like to find the minimum period, since every other period is a multiple of that, according to a theorem I'm not proving.)

Theorem 1. *Let m be a positive integer. The remainders of D_n modulo m repeat every $2m$ terms, and if $m = 1$ or m is even they repeat every m terms.*

That is, m or $2m$ is a period of $D_n \bmod m$. I'm not saying there is not a shorter period. That's still open—any takers?

Proof. We have several equations involving D_n. The ones that are useful here are

$$D_n = nD_{n-1} + (-1)^n \tag{1}$$

and

$$D_n = (n-1)(D_{n-1} + D_{n-2}). \tag{2}$$

If we look at these equations modulo m, we notice a couple of things.

First:

If $n \equiv 0 \bmod m$, then $D_n \equiv (-1)^n \bmod m$.

This follows from Equation (1), since $n \equiv 0 \bmod m$ implies $nD_{n-1} \equiv 0$. (If n is a multiple of m, then so is nD_{n-1}.) Thus, for any integer $k \geq 0$,

$$D_{km} \equiv 1 \qquad \text{when } m \text{ is even,} \tag{3}$$

$$D_{km} \equiv \begin{cases} 1 & \text{if } k \text{ is even,} \\ -1 & \text{if } k \text{ is odd,} \end{cases} \qquad \text{when } m \text{ is odd.} \tag{4}$$

(Note that $-1 \equiv m - 1 \bmod m$.)

Second:

If $n \equiv 1 \bmod m$, then $D_n \equiv 0 \bmod m$.

This follows from Equation (2), since $n \equiv 1 \bmod m$ implies $n-1 \equiv 0 \bmod m$, which implies $(n-1)(D_{n-1}+D_{n-2}) \equiv 0 \bmod m$. We get, for any integer $k \geq 0$,

$$D_{km+1} \equiv 0 \bmod m. \tag{5}$$

Now I will prove the theorem. Let's compare D_n to D_{n+2m} first. Using (1) we deduce that

$$D_n \equiv nD_{n-1} + (-1)^n \qquad \bmod m$$

and

$$D_{n+2m} \equiv (n+2m)D_{n-1+2m} + (-1)^{n+2m} \equiv nD_{(n-1)+2m} + (-1)^n \qquad \bmod m,$$

because $n+2m \equiv n \bmod m$. (Meaning: $n+2m$ and n have the same remainders upon division by m; so $(n+2m)D_{n-1+2m}$ and nD_{n-1+2m} also have the same remainders.) So, if $D_{n-1} \equiv D_{(n-1)+2m} \bmod m$, then $D_n \equiv D_{n+2m} \bmod m$. But this is just what we need for induction, provided we get the base case.

The base case is $n = 1$. By Equation (5), $D_1 \equiv 0 \equiv D_{2m+1} \bmod m$. Therefore, by induction on n, $D_n \bmod m$ has a period $2m$ for all $n \geq 1$.

We still need to check that $D_0 \equiv D_{2m}$. By Equations (3) and (4), $D_{2m} \equiv 1 \equiv D_0 \bmod m$.

That concludes the proof that $2m$ is a period.

Now I prove that m is a period when m is even. It's almost the same proof. Compare D_n to D_{n+m}. Using (1) we deduce that

$$D_n \equiv nD_{n-1} + (-1)^n \qquad \bmod m$$

and

$$D_{n+m} \equiv (n+m)D_{n-1+m} + (-1)^{n+m} \equiv nD_{(n-1)+m} + (-1)^n \qquad \bmod m,$$

because m is even. So, if $D_{n-1} \equiv D_{(n-1)+m} \bmod m$, then $D_n \equiv D_{n+m} \bmod m$. This is what we need for induction, provided we get the base case and the lowest case.

The base case is $n = 1$. By Equation (5), $D_1 \equiv 0 \equiv D_{m+1} \bmod m$. Therefore, by induction on n, $D_n \bmod m$ has a period m for all $n \geq 1$.

We still need to check that $D_0 \equiv D_m$. By Equation (3), $D_m \equiv 1 \equiv D_0 \bmod m$.

That concludes the proof that m is a period for even numbers m.

One more thing to prove: The case $m = 1$. Every number has the same remainder modulo 1, namely, 0. So, $D_n \bmod 1$ is just an infinite sequence of 0's, giving a period of 1. (Easy!) □

Reminder: I haven't proved that m or $2m$ is the *minimum* period.