Megoldás. 1. eset. A cikkben leírt eljáráshoz hasonlóan számozzuk a lapokat – felülről lefelé haladva – a $0, 1, 2, \ldots, 51$ sorszámokkal. A kezdetben legelső és legutolsó kártya mindig a helyén marad, egyébként egy keverés után a k-adik lap arra az y_k-adik helyre kerül, amelyre $y_k \equiv 2k \pmod{51}$ ($k = 1, 2, \ldots, 50$). Ha n-szer egymás után keverünk, akkor tehát az eredetileg k-as sorszámú kártya a $2^n k$-adik helyre kerül $\pmod{51}$. Akkor lesz mindegyik lap az eredeti helyén, ha minden $k = 1, 2, \ldots, 50$-re $2^n k \equiv k \pmod{51}$ teljesül, azaz $2^n \equiv 1 \pmod{51}$. A 2 hatványait modulo 51 egymás után felírva:

$$\begin{aligned} 2^1 &\equiv 2 \pmod{51}, & 2^5 &\equiv 32 \pmod{51}, \\ 2^2 &\equiv 4 \pmod{51}, & 2^6 &\equiv 64 \equiv 13 \pmod{51}, \\ 2^3 &\equiv 8 \pmod{51}, & 2^7 &\equiv 2 \cdot 13 = 26 \pmod{51}, \\ 2^4 &\equiv 16 \pmod{51}, & 2^8 &\equiv 2 \cdot 26 = 52 \equiv 1 \pmod{51}; \end{aligned}$$

ezek szerint $n = 8$ az a legkisebb szám, amelyre ez megvalósul, vagyis a nyolcadik keverés után áll vissza először az eredeti sorrend.

2. eset. Most úgy tudjuk a legkönnyebben nyomon követni a kártyák mozgását, ha a lapokat 1-től 52-ig számozzuk. Ekkor a k-adik lap a $2k$-adik helyre kerül $\pmod{53}$, az n-edik keverés után tehát a $2^n k$-adikra $\pmod{53}$. Ezúttal tehát azt a legkisebb n értéket keressük, amelyre $2^n \equiv 1 \pmod{53}$. A 2 hatványait sorban felírva $\pmod{53}$ elég sokáig kellene várnunk, amíg az 1 először felbukkan. Meggyorsíthatja a számolást, ha leszűkítjük azon n számok körét, amelyek szóba jöhetnek. Mivel 53 prímszám, a kis Fermat-tétel szerint $2^{52} \equiv 1 \pmod{53}$, azért a 2 hatványai modulo 53 periodikusan ismétlődnek, és a periódus hossza 52. Feladatunk a *legkisebb* periódus (jelölje azt p) megtalálása, mivel arra egyrészt $2^p \equiv 2^{p-p} = 1 \pmod{53}$ – vagyis $n \leq p$ –, másrészt $2^n \equiv 1 \pmod{53}$ miatt a 2 hatványai periodikusak modulo 53, így $p \leq n$; tehát valóban $p = n$. A legkisebb periódus minden periódusnak, így 52-nek is osztója, azaz csak 1, 2, 4, 13, 26 vagy 52 lehet. Tekintsük a következő 2-hatványokat:

$$\begin{aligned} 2^4 &\equiv 16 \pmod{53}, \\ 2^8 \equiv 16^2 &= 256 \equiv -9 \pmod{53}, \\ 2^{16} \equiv (-9)^2 &= 81 \equiv 28 \pmod{53}, \end{aligned}$$

ezért

$$2^{26} = 2^{16} \cdot 2^8 \cdot 2^2 \equiv 28 \cdot (-9) \cdot 4 \equiv 6 \cdot (-9) = -54 \equiv -1 \not\equiv 1 \pmod{53}.$$

Ez azt jelenti, hogy 26 nem periódus, ezért 13 sem, az 1, 2, 4 pedig nyilván nem az. Tehát a legrövidebb periódus 52, vagyis az eredeti sorrend először az ötvenkettedik keverés után áll vissza.