The Parity of a Permutation
(Chapter 6, Nos. 32 & 36)

The only difference is that # 32 is about cyclic permutations (one cycle) and # 36 is about any permutation. It turns out that the same proof idea works for both problems. Some of the details are different.

I'll remind you of the definition of parity and of the alternate language for parity of a permutation p. Let $i(p)$ denote the number of inversions in p. (Remember that an inversion is a pair (p_i, p_j) in p where $i < j$ but $p_i > p_j$.) Thus, the *parity* of p is defined to be the parity of $i(p)$. The *sign* of p is

$$\operatorname{sgn}(p) := (-1)^{i(p)}.$$

Obviously, the parity is even if and only if the sign is $+1$. I'll use the sign instead of the parity because that notation seems to fit the proof better.

Theorem 0.1. *The sign of a permutation of $[n]$ that has k cycles is $(-1)^{n-k}$.*

Isn't this remarkable? Would you have thought the sign (or parity) was so simple? It's not that easy to prove, but not that hard, either.

Proof. I'll use induction on n. The cases $n \leq 2$ are trivial. (For $n = 0$, necessarily $k = 0$ and $i(p) = 0$ so it works. That's a weird case and if you don't believe in it, it's okay!)

So let's assume we know the theorem for $n - 1$, where $n \geq 3$, and we want to prove it for n. We take a permutation $p \in S_n$ and let k be the number of cycles in p.

Case 1. (n) is a cycle in p. Then deleting n, we have a permutation q of $[n-1]$ which has $k - 1$ cycles (since (n) was a cycle by itself). By the induction hypothesis,

$$\operatorname{sgn}(q) = (-1)^{(n-1)-(k-1)} = (-1)^{n-k}. \tag{0.1}$$

Now, I prove that $i(p) = i(q)$. Look at the two-line notations for p and q.

$$p = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ p_1 & p_2 & \dots & p_{n-1} & n \end{pmatrix}; \qquad q = \begin{pmatrix} 1 & 2 & \dots & n-1 \\ p_1 & p_2 & \dots & p_{n-1} \end{pmatrix}.$$

The value $p_n = n$ doesn't participate in any inversions, so $i(q) = i(p)$. Therefore, $\operatorname{sgn}(p) = \operatorname{sgn}(q)$. Combined with (0.1), we get

$$\operatorname{sgn}(p) = (-1)^{i(p)} = (-1)^{i(q)} = (-1)^{n-k}.$$

That proves Case 1.

Case 2. n belongs to a cycle of length $l \geq 2$ in p. Let's write the cycle as $(H \ \cdots \ J \ n)$. When we delete n from p, giving q, we get the cycle $(H \ \cdots \ J)$ in q, while all other cycles are the same in p and q. Thus, q has k cycles, just like p. (If the cycle with n has length 2, H and J are the same. That doesn't affect the proof—you should check that!)

In two-line notation p and q are

$$p = \begin{pmatrix} 1 & 2 & \dots & J & J+1 & \dots & n-1 & n \\ p_1 & p_2 & \dots & n & p_{J+1} & \dots & p_{n-1} & H \end{pmatrix};$$

$$q = \begin{pmatrix} 1 & 2 & \dots & J & J+1 & \dots & n-1 \\ p_1 & p_2 & \dots & H & p_{J+1} & \dots & p_{n-1} \end{pmatrix}.$$

The only differences between p and q are in column J and in the extra column n. Let $g :=$ the number of values p_j in columns $j = J+1, J+1, \ldots, n-1$ such that $p_j > H$; then there are $(n-1-J)-g$ values p_j in those columns such that $p_j < H$.

Let's examine all the inversions. An inversion, or non-inversion, in p that doesn't involve n or H is an inversion, or non-inversion, in q, the same as in p. A pair (p_i, n) in p, where $i < J$, can't be an inversion in p. A pair $(p_i, p_n) = (p_i, H)$ in p where $i < J$ becomes a pair $(q_i, q_J) = (p_i, H)$ in q, and it is an inversion in q if and only if it was an inversion in p. Thus, the only changes in the set of inversions between p and q are:

(1) Pairs (n, p_j), from column J and column j in p, where $J < j \leq n$. We have the pair $(p_J, p_j) = (n, p_j)$ in p, which is always an inversion, so we get $n - J$ inversions in p. They don't correspond to any pairs in q, since n doesn't appear in q.

(2) Pairs (p_j, H), from column j and column n in p, where $J < j < n$. We have the pair $(p_j, p_n) = (p_j, H)$ in p, which is an inversion if and only if $p_j > H$. This corresponds to the pair $(q_J, q_j) = (H, p_j)$ in q, which is an inversion if and only if $p_j \not> H$. Thus, we lose g inversions from p but we gain $(n-1-J)-g$ inversions in q, for a net gain of $(n-1-J)-2g$ inversions.

Thus, as we change from p to q we lose $(n-J)+g$ inversions and gain $(n-1-J)-g$ inversions, for a net loss of $(n-J)-[(n-1-J)-2g] = 2g+1$ inversions; that is, $i(p) = i(q) + (2g+1)$. The number of inversions changes by an odd number. That implies $\operatorname{sgn}(p) = (-1)\operatorname{sgn}(q) = (-1)(-1)^{(n-1)-k} = (-1)^{n-k}$ by the induction hypothesis.

Thus, the induction is valid in both cases. It follows that the theorem is true for all n. $\square$