Piotrland

In Piotrland there are no kings or queens, but there are a different tribes. A council sits on a circular table that has p seats, where p is a prime number. Councils can be formed by people from different tribes, but councils cannot be all composed of any one single tribe. How many possible councils are there?

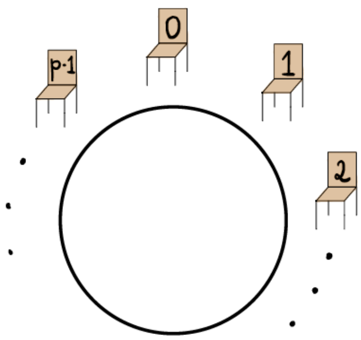

Figure 1: Seats around the table.

Solution Let us number the p seats around the table from 0 to $p-1$ as shown on Figure 1. We use tuples $x = (x_0, x_1, \dots x_{p-1})$ to represent seatings where x_i = tribe of person sitting at seat i. Note that two seatings $x \neq y$ can correspond to the same council! We call a seating valid if at least two tribes are present. For $n \geq 0$ let $R(x, n)$ be the tuple we get after n clockwise rotations of x, i.e. $R(x, 1) = (x_1, x_2, \dots x_{p-1}, x_0)$ and $R(x, 2) = (x_2, x_3, \dots x_{p-1}, x_0, x_1)$ et cetera (see Figure 2).

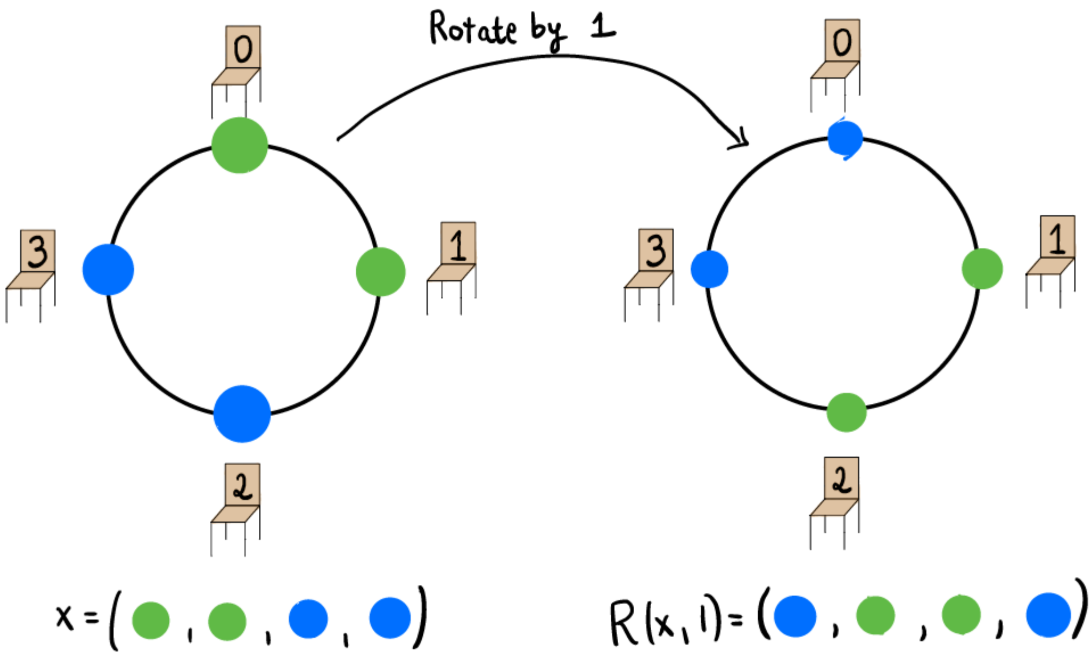

Figure 2: Rotating a seating by 1.

Finally, for a seating x let S_x be the *orbit* of x defined as

$$S_x := \{R(x,n) \,:\, n \geq 0\}.$$

In other words, S_x is the set of seatings one can obtain by rotating x. See Figure 3 for an example.

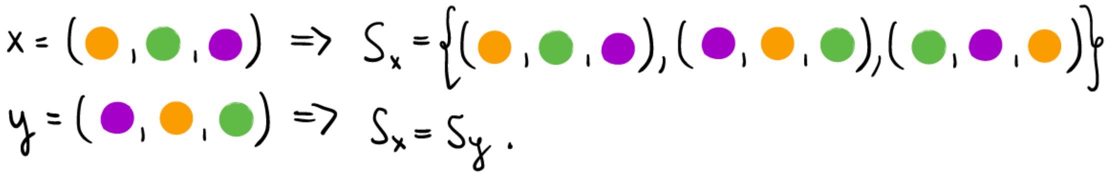

Figure 3: Example of an orbit.

Lemma 1 — *For a valid seating x and $n \geq 0$ we have $R(x,n) = x$ if and only if $n \equiv 0 \,(mod\ p)$.*

Remark 1. Notice that rotations by $n \geq 0$ where $n \equiv 0 \,(\text{mod } p)$ are precisely the full rotations of the table: if $n = 0$ then you don't rotate, if $n = p$ then you fully rotate once, if $n = k \cdot p$ you fully rotate k times. Thus, $R(x, kp) = x$ is not saying much. However, the lemma says that $R(x,n) = x$ can happen *only if* $n = k \cdot p$ for some k.

Proof. Suppose that $R(x,n) = x$. Looking at the first entry of the two tuples this gives

$$x_{n \,(\text{mod } p)} = x_0.$$

Note that clearly $x = R(x,n) = R(R(x,n),n) = R(x,2n)$. Continuing like this, by induction, $x = R(x, k \cdot n)$ for all $k \geq 0$. We have shown that

$$x_0 = x_{n (\text{mod } p)} = x_{2n (\text{mod } p)} = x_{3n (\text{mod } p)} = \dots. \tag{1}$$

If $n \equiv 0$ (mod p) this just says that $x_0 = x_0 = x_0 = \dots$. If $n \not\equiv 0$ (mod p) however, then n and p are relatively prime, and thus

$$\{0, n \,(\text{mod } p), 2n \,(\text{mod } p), (p-1)n \,(\text{mod } p)\} = \{0, 1, 2, \dots p-1\}.$$

For example, for $p = 5$ and $n = 7$

$$\{0, 7 \,(\text{mod } 5), 2 \cdot 7 \,(\text{mod } 5), 3 \cdot 7 \,(\text{mod } 5), 4 \cdot 7 \,(\text{mod } 5)\} = \{0, 2, 4, 1, 3\} = \{0, 1, 2, 3, 4\}.$$

We see now from equation (1) that $n \not\equiv 0 \,(\text{mod } p)$ would contradict the fact that x is a valid seating. Therefore the only possibility is to have $n \equiv 0$ (mod p). ☐

What Lemma 1 tells us is that

$$|S_x| = p \tag{2}$$

for all valid seatings x. Indeed, by its definition the orbit of x is

$$S_x = \{x, R(x,1), R(x,2), \dots R(x, p-1)\}$$

and the elements on the RHS above are all distinct by Lemma 1. Don't be fooled by the simplicity of the fact (2). It only works because p was prime! See Figure 4 for a counterexample when $p = 4$.

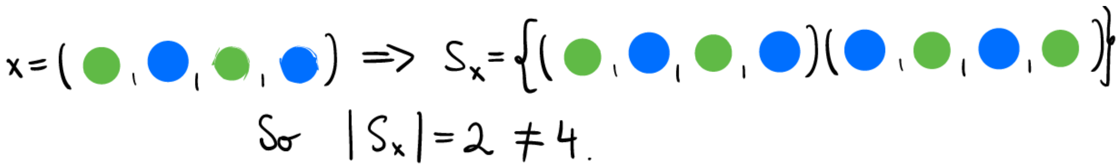

Figure 4: Example of an orbit with $|S_x| \neq p$.

Recall that our goal is to count the number of councils that can be formed. The crucial observation is that

$$\text{number of councils } = \text{number of distinct orbits} = |\{S_x \, : \, x \text{ is a valid seating}\}|.$$

For two valid seatings x, y it is easy to see that either $S_x = S_y$ or $S_x \cap S_y = \varnothing$. In other words, the distinct orbits form a partition of the set of valid seatings. Take valid seatings $x^{(1)}, x^{(2)}, \ldots x^{(l)}$ such that their orbits $S_{x^{(1)}}, \ldots S_{x^{(l)}}$ are distinct and

$$\bigcup_{i=1}^{l} S_{x^{(i)}} = \{\text{all valid seatings}\}.$$

Note that necessarily $l =$ number of distincts orbits $=$ number of councils. Taking the cardinality of both sets, we obtain

$$\left| \bigcup_{i=1}^{l} S_{x^{(i)}} \right| = \text{number of valid seatings.} \tag{3}$$

We know that for disjoint sets A, B we have $|A \cup B| = |A| + |B|$ so that the LHS above is

$$\left| \bigcup_{i=1}^{l} S_{x^{(i)}} \right| = \sum_{i=1}^{l} |S_{x^{(i)}}| = l \cdot p.$$

What remains is counting the number of valid seatings. But this is easy! There are p seats and a tribes, so in total there are a^p seatings. However, a of these are invalid because only one tribe is present. Therefore, in total there are $a^p - a$ valid seatings. Putting everything together, plugging into equation (3) we get

$$l \cdot p = a^p - a,$$

so that our final answer is

$$\text{number of councils} = \frac{a^p - a}{p}.$$

Concluding remarks In the process of solving the problem we actually proved a well known theorem in number theory, namely Fermat's Little Theorem. More generally, you may wonder what happens to our solution if p is not prime. This more difficult case can be tackled with a slight generalization of our argument above which is known as Burnside's Lemma, an awesome theorem from the field of Group Theory.