Counters (mod m) on an n-gon

Samuel Korsky

November 11, 2021

Abstract

We consider a game in which a blindfolded player attempts to set n counters lying on the vertices of a rotating regular n-gon table simultaneously to 0. When the counters count (mod m) we show that the player can win if and only if $n = 1$, $m = 1$, or $(n, m) = (p^a, p^b)$ for some prime p and $a, b \in \mathbb{N}$. We also extend the result to any subset of the symmetric group $S \subseteq S_n$, with the original formulation corresponding to $S = \mathbb{Z}_n$ (rotations of the table).

1 Introduction

We start with a well-known brainteaser: four coins lie on the corners of a square table, some heads-up and some tails-up (they may all have the same orientation). Each turn, a blindfolded player can flip some of the coins, after which the table is rotated arbitrarily. If the player's goal is to at any time have all coins heads-up simultaneously, does he have a strategy that guarantees victory?

Note that the simple strategy of flipping one coin at random each turn wins eventually with probability 1. However, the question we consider here is whether the player has a strategy guaranteed to win within a finite number of turns; and indeed, for the simple case above there is a strategy that wins within 15 turns!

In particular, label the positions of the table $1, 2, 3, 4$. Then a *move* (performed once per turn) will consist of a vector in $\mathbb{Z}_2^4$, with 0 denoting leaving the coin in the corresponding position as is and 1 denoting flipping the coin in that position. E.g., the vector $(0, 0, 0, 1)$ denotes only flipping the coin in position 4. The player's strategy should then be the following sequence of 15 moves:

$$(1,1,1,1),(0,1,0,1),(1,1,1,1),(0,0,1,1),(1,1,1,1),(0,1,0,1),(1,1,1,1),(0,0,0,1),$$
$$(1,1,1,1),(0,1,0,1),(1,1,1,1),(0,0,1,1),(1,1,1,1),(0,1,0,1),(1,1,1,1)$$

To show that this strategy wins, we perform casework on the starting configuration of the four coins. Note that if all four coins start heads-up the player wins instantly, so we will ignore this case. We will ignore rotation when discussing each possible configuration of coins after a set of moves has been performed.

Case 1: All four coins start tails-up. In this case the player will win after the first move of $(1, 1, 1, 1)$.

Case 2: Two diagonally opposite coins start heads-up and the other two coins start tails-up. In this case, the first move of $(1, 1, 1, 1)$ does not affect the configuration, and the second move forces all coins to be oriented in the same way. If this orientation happens to be tails, the player will win after his third move of $(1, 1, 1, 1)$.

Case 3: Two adjacent coins start heads-up and the other two coins start tails up. In this case the first three moves don't affect the configuration, and then the fourth move necessarily brings us to either the configuration in Case 1 or Case 2, after which the analysis follows similarly.

Case 4: Three coins have the same orientation, and the fourth coin has the opposite orientation. In this case the first seven moves don't affect the configuration, and then the eighth move necessarily brings us to one of the configurations in Cases 1, 2, or 3, after which the analysis follows similarly.

One naturally asks the question, what if instead of four coins there were n coins? Furthermore, viewing a coin as a counter counting $\pmod 2$ (to which the player adds either 0 or 1 each turn), what if instead the counters counted $\pmod m$, with the player adding one of $0, 1, \ldots m-1$ to each counter each turn? In general, we shall show the following:

Theorem 1.1. The player can win if and only if $n = 1$, $m = 1$, or $(n, m) = (p^a, p^b)$ for some prime p and $a, b \in \mathbb{N}$.

Our proof consists of four separate parts. First, we will show that if $(n, m) = (p, q)$ for distinct primes p, q then the player cannot win. Then we shall show if the player cannot win if $(n, m) = (a, b)$ then the player also cannot win for $(n, m) = (a, bk)$ or $(n, m) = (ak, b)$ for any $k \in \mathbb{N}$. The combination of these two facts will show that the player can only win if $n, m > 1$ are powers of the same prime. Then we will constructively show that the player can win if $(n, m) = (p^a, p)$ for a prime p and any $a \in \mathbb{N}$. Finally, we will extend the construction to prove the full theorem.

2 The $(n, m) = (p, q)$ case

We start by extending the notation in the introduction. Instead of denoting "moves" by vectors in $\mathbb{Z}_2^4$, we will now use vectors in $\mathbb{Z}_m^n$. E.g., the vector $(2, 0, 3)$ will denote adding 2 to the counter in position 1 and adding 3 to the counter in position 3. We will also use vectors in $\mathbb{Z}_m^n$ to describe the configuration of counters. Furthermore, call a configuration of counters *homogenous* if each counter on the table shows the same number, and non-homogenous otherwise.

Lemma 2.1. The player cannot win if $(n, m) = (p, q)$ for distinct primes p, q.

Proof. When $(n, m) = (p, q)$ for distinct primes p, q, we will show that for any non-homogenous configuration, there is no move guaranteed to make the configuration homogenous following an arbitrary rotation of the regular n-gon table.

Indeed, suppose the configuration on the table prior to a rotation was $(x_1, x_2, \ldots, x_p)$ and consider any move $(y_1, y_2, \ldots, y_p)$. For this move to guarantee that the configuration of the table afterwards was homogenous, the following equalities would have to hold simultaneously:

$$\begin{aligned}
x_1 + y_1 = x_2 + y_2 = \cdots = x_p + y_p \pmod q \\
x_2 + y_1 = x_3 + y_2 = \cdots = x_1 + y_p \pmod q \\
\vdots \\
x_p + y_1 = x_1 + y_2 = \cdots = x_{p-1} + y_p \pmod q.
\end{aligned}$$

This implies that

$$x_1 - x_2 = x_2 - x_3 = \cdots = x_p - x_1 = y_2 - y_1 \pmod q.$$

Thus

$$p(x_1 - x_2) = (x_1 - x_2) + (x_2 - x_3) + \cdots + (x_p - x_1) = 0 \pmod q$$

and so $x_1 = x_2 \pmod q$. Similarly we obtain $x_1 = x_2 = \cdots = x_p \pmod q$ so indeed such a move is only possible if the configuration of the table was already homogenous.

Therefore if the starting configuration is non-homogenous, the player can never force the configuration to be homogenous and so cannot win. ■

3 The $(n, m) = (ak, b)$ and $(n, m) = (a, bk)$ cases

We handle each case separately:

Lemma 3.1. If the player cannot win when $(n, m) = (a, b)$, then the player cannot win when $(n, m) = (ak, b)$ for any $k \in \mathbb{N}$.

Proof. Suppose that the player cannot win if $(n, m) = (a, b)$ for some $(a, b) \in \mathbb{N}^2$, and consider the case where $(n, m) = (ak, b)$ for some $k \in \mathbb{N}$. Suppose for the sake of contradiction that the player had a sequence of moves $y_1, y_2, \ldots, y_N$ for some $N \in \mathbb{N}$ that guaranteed a win, where $y_i = (y_{i,1}, y_{i,2}, \ldots, y_{i,ak})$ for all i. Now let $y_i' = (y_{i,k}, y_{i,2k}, \ldots, y_{i,ak})$ for all i. We must have that the sequence of moves $y_1', y_2', \ldots, y_N'$ wins for $(n, m) = (a, b)$, contradiction. ■

Lemma 3.2. If the player cannot win when $(n, m) = (a, b)$, then the player cannot win when $(n, m) = (a, bk)$ for any $k \in \mathbb{N}$.

Proof. Suppose that the player cannot win if $(n, m) = (a, b)$ for some $(a, b) \in \mathbb{N}^2$, and consider the case where $(n, m) = (a, bk)$ for some $k \in \mathbb{N}$. Suppose for the sake of contradiction that the player had a sequence of moves $y_1, y_2, \ldots, y_N$ for some $N \in \mathbb{N}$ that guaranteed a win, where $y_i = (y_{i,1}, y_{i,2}, \ldots, y_{i,a})$ for all i. Note that $y_{i,j} \in \mathbb{Z}_{bk}$ for all i, j, and define the homomorphism $\phi : \mathbb{Z}_{bk} \to \mathbb{Z}_b$ where $\phi(x) = x \pmod b$. Now let $y_i' = (\phi(y_{i,1}), \phi(y_{i,2}), \ldots, \phi(y_{i,a}))$ for all i. We must have that the sequence of moves $y_1', y_2', \ldots, y_N'$ wins for $(n, m) = (a, b)$, contradiction. ■

Corollary 3.3. The combination of Lemmas 2.1, 3.1, and 3.2 immediately imply the "only if" direction in Theorem 1.1.

4 The $(n, m) = (p^a, p)$ case

Here we prove the following lemma constructively:

Lemma 4.1. The player can win if $(n, m) = (p^a, p)$ for some prime p and $a \in \mathbb{N}$.

Proof. Let $x_{i,j} = \binom{i}{j} \pmod p$ where $x_{i,j} \in \mathbb{Z}_p$ for all i, j. Furthermore, let $x_j = (x_{0,j}, x_{1,j}, \ldots, x_{p^a-1,j})$ for all $j \in \{0, 1, \ldots, p^a - 1\}$. For all $i \in \{1, 2, \ldots, p^{p^a} - 1\}$, let $y_i = x_{v_p(i)}$ where v_p denotes p-adic valuation. We claim that the sequence of moves $y_1, y_2, \ldots, y_{p^{p^a}-1}$ wins.

Since the matrix $[x_0^T \ x_1^T \ \ldots \ x_{p^a-1}^T]$ is lower triangular and its main diagonal is identically 1, its determinant is $1 \neq 0$ and so the moves $x_0, x_1, \ldots, x_{p-1}$ form a basis over $\mathbb{Z}_p^{p^a}$. Therefore, we can write the starting configuration s as $s = c_0x_0 + c_1x_1 + \ldots c_{p^a-1}x_{p^a-1}$ for some $c_0, c_1, \ldots, c_{p^a-1} \in \mathbb{Z}_p$.

The following intermediate lemma is then the key to the proof:

Lemma 4.2. For any j, let x_j' be a cyclic permutation of x_j. Then $x_j - x_j' = e_0x_0 + e_1x_1 + \cdots + e_{j-1}x_{j-1}$ for some $e_0, e_1, \ldots, e_{j-1} \in \mathbb{Z}_p$.

Proof. We proceed by induction on j. When $j = 0$ the result is trivial, since $x_j = x_j'$. Now suppose $j > 0$ and let $x_j^{(k)} = (x_{k,j}, x_{k+1,j}, \ldots, x_{k-1,j})$ for all $k \in \{0, 1, \ldots, p^a - 1\}$, so that $x_j^{(0)} = x_j$. Repeatedly utilizing the fact that $\binom{i}{j} - \binom{i-1}{j} = \binom{i-1}{j-1}$ and $\binom{p^a}{j} = \binom{0}{j} = 0 \pmod p$ we have that, working in $\mathbb{Z}_p^{p^a}$,

$$\begin{aligned}
x_j^{(k+1)} - x_j^{(k)} &= (x_{k+1,j}, x_{k+2,j}, \ldots, x_{k,j}) - (x_{k,j}, x_{k+1,j}, \ldots, x_{k-1,j}) \\
&= (x_{k,j-1}, x_{k+1,j-1}, \ldots, x_{k-1,j-1}) \\
&= x_{j-1}^{(k)}
\end{aligned}$$

Therefore letting $x'_j = x_j^{(k)}$ for some k we have

$$\begin{aligned} x'_j - x_j &= \left(x_j^{(k)} - x_j^{(k-1)}\right) + \left(x_j^{(k-1)} - x_j^{(k-2)}\right) + \cdots + \left(x_j^{(1)} - x_j^{0)}\right) \\ &= x_{j-1}^{(k-1)} + x_{j-1}^{(k-2)} + \cdots + x_{j-1}^{(0)} \end{aligned}$$

But by the inductive hypothesis we know that each $x_{j-1}^{(i)}$ can be written as a linear combination of $x_0, x_1, \ldots, x_{j-1}$ (with a coefficient of 1 behind x_{j-1}), which completes the proof. ■

Returning to the proof of Lemma 4.1, recall that we wrote $s = c_0x_0 + c_1x_1 + \ldots c_{p^a-1}x_{p^a-1}$ for some $c_0, c_1, \ldots, c_{p^a-1} \in \mathbb{Z}_p$. For any such starting configuration s, let $f(s)$ denote that largest i such that $c_i \neq 0$. We will show by induction on $f(s)$ that the sequence of moves $y_1, y_2, \ldots, y_{p^{f(s)+1}-1}$ wins. Note that the base case where $c_i = 0$ for all i is trivial, since the player immediately wins.

The main idea is that as a consequence of Lemma 4.2, every time the table rotates and we rewrite the new configuration as a linear combination of $x_0, x_1, \ldots, x_{p^a-1}$, the coefficient behind $x_{f(s)}$ is invariant. Specifically, suppose $c_{f(s)} = c \neq 0$. Let s' be the configuration on the table after $(p-c)p^{f(s)}$ moves, and write $s' = c'_0x_0 + c'_1x_1 + \ldots c'_{p^a-1}x_{p^a-1}$ for some $c'_0, c'_1, \ldots, c'_{p^a-1} \in \mathbb{Z}_p$. By Lemma 4.2, each move y_i with $v_p(i) < f(s)$ would not affect any of the coefficients behind x_j for any $j \geq f(s)$ and each of the $p-c$ moves with $v_p(i) = f(s)$ would increase the coefficient behind $x_{f(s)}$ by 1 regardless of how the table rotates between moves, so that $c'_{f(s)} = c_{f(s)} + p - c = 0 \pmod p$. Therefore after $(p-c)p^{f(s)}$ moves we are in a configuration with $f(s') < f(s)$ and since the next $p^{f(s')+1} - 1$ moves are copies of the first $p^{f(s')+1} - 1$ moves, we are done by induction. ■

5 The $(n, m) = (p^a, p^b)$ case

Finally, we expand upon our construction in Section 4 to prove Theorem 1.1 in its entirety. Specifically, we will show by induction on b that there is a sequence of $p^{bp^a} - 1$ moves that wins. The base case of $b = 1$ follows from the proof of Lemma 4.1.

Now, suppose $x_1, x_2, \ldots, x_{p^{(b-1)p^a}-1}$ is a sequence of moves that wins in the $(n, m) = (p^a, p^{b-1})$ case. Additionally, let $y_1, y_2, \ldots, y_{p^{p^a}-1}$ be the sequence of moves that wins in the $(n, m) = (p^a, p)$ case as in the proof of Lemma 4.1. Note that $x_i \in \mathbb{Z}_{p^{b-1}}^{p^a}$ for all i and $y_j \in \mathbb{Z}_p^{p^a}$ for all j, but interpret each of these vectors as vectors in $\mathbb{Z}_{p^b}^{p^a}$ (through the identity homomorphism). Define the homomorphism $\varphi : \mathbb{Z}_{p^b}^{p^a} \to \mathbb{Z}_{p^{b-1}}^{p^a}$ where $\varphi(x) = x \pmod{p^{b-1}}$ element-wise, and let

$$z_i = \begin{cases} px_{\varphi(i)} & \text{if } i \neq 0 \\ y_{ip^{(1-b)p^a}} & \text{if } i = 0 \end{cases} \pmod{p^{(b-1)p^a}}$$

for all $i \in \{1, 2, \ldots, p^{bp^a} - 1\}$, where $px_{\varphi(i)}$ denotes element-wise multiplication by p. We claim that $z_1, z_2, \ldots, z_{p^{bp^a}-1}$ is a sequence of moves that wins in the $(n, m) = (p^a, p^b)$ case.

If we consider the configuration of the table $\pmod p$, then up to rotation none of the moves of the form $px_{\varphi(i)}$ affect the configuration. Therefore we know by the definition of the sequence $y_1, y_2, \ldots, y_{p^{p^a}-1}$ that after some move of the form y_j, every counter will be $0 \pmod p$. It is then clear that after this move y_j, the following sequence of $p^{(b-1)p^a} - 1$ moves $px_1, px_2, \ldots, px_{p^{(b-1)p^a}-1}$ will win the game. This completes the proof of Theorem 1.1. ■

We will also prove that our constructions are optimal in terms of number of moves necessary to win.

Theorem 5.1. If the player can win for a given (n, m), then he can guarantee a win in no less than $m^n - 1$ moves.

Proof. Consider any sequence of moves $y_1, y_2, \dots, y_N \in \mathbb{Z}_m^n$ with $N < m^n - 1$. Let $z_k = \sum_{i=1}^{k} y_i$ for all $k \in \{1, 2, \dots, N\}$ and suppose that the table did not rotate at all after any of the moves. Then this sequence of moves would only win if the starting configuration was equal to 0 or $-z_k$ (with each element reduced $\pmod{m}$) for some k. But there are $N+1 < m^n$ such winning configurations and m^n possible starting configurations, so there are a non-zero number of starting configurations for which this sequence of moves never wins. This implies the desired result. ■

6 Generalizing to groups

Instead of the table simply rotating, one can imagine that the table permutes the counters in positions $1, 2, \dots, n$ based on elements from some subset $S \subseteq S_n$, where S_n denotes the symmetric group and where S contains the identity.[1] Denote the parameters of this game as (S, m), so that $(\mathbb{Z}_n, m)$ represents the setting discussed in the previous sections. Additionally, let $G \leq S_n$ be the subgroup of S_n generated by S. We present our main result:

Theorem 6.1. The player can win the (S, m)-game if and only if $|G| = 1$, $m = 1$, or $(|G|, m) = (p^a, p^b)$ for some prime p and $a, b \in \mathbb{N}$.

We break the proof into two sections: first we shall show the "only if" direction, and then we shall show the "if" direction when $b = 1$. The case where $b > 1$ then follows immediately from the logic in the proof of Theorem 1.1 in Section 5.

Lemma 6.2. The player can win the (S, m)-game only if $|G| = 1$, $m = 1$, or $(|G|, m) = (p^a, p^b)$ for some prime p and $a, b \in \mathbb{N}$.

Proof. We mimic the proof of Lemma 2.1. Suppose that there exist distinct primes p and q with $v_p(|G|), v_q(m) > 0$ and without loss of generality assume $m = q$. By Cauchy's Theorem there must exist some $c \in G$ with order p. Let $g(x)$ denote the position of the counter currently at position x after the permutation $g \in G$ is applied to the counters on the table. Call a configuration of the table *semi-homogenous* if the counters in positions $g(1), gc(1), gc^2(1), \dots, gc^{p-1}(1)$ show the same number for all $g \in G$. We will show that for any non-semi-homogenous configuration on the table, there is no move guaranteed to make the configuration semi-homogenous following an arbitrary permutation of the table.

Indeed, suppose the configuration on the table prior to a permutation was $(x_1, x_2, \dots, x_n)$ and consider any move $(y_1, y_2, \dots, y_n)$. For convenience, let x_g denote $x_{g(1)}$ for all $g \in G$ and define y_g similarly, and let us work in $\mathbb{Z}_q$. For this move to guarantee that the configuration of the table was semi-homogenous after the move, the following $|S||G|$ strings of equalities would have to hold simultaneously:

$$x_{sg} + y_g = x_{sgc} + y_{gc} = \cdots = x_{sgc^{p-1}} + y_{gc^{p-1}}$$

for all $s \in S$ and $g \in G$. Now, fix a specific $d \in G$ and write $dcd^{-1} = \prod_{i=1}^{k} s_i$ for some $k \in \mathbb{N}$ and $s_1, s_2, \dots, s_k \in S$ (this representation is guaranteed to exist since S generates G). Using the first equality in the string with $g = d$ and $s \in \{1, s_k\}$, we obtain $x_d - x_{dc} = x_{s_k d} - x_{s_k dc} = y_{dc} - y_d$. Using the first equality again with $g = s_k d$ and $s \in \{1, s_{k-1}\}$ we obtain $x_{s_k d} - x_{s_k dc} = x_{s_{k-1} s_k d} - x_{s_{k-1} s_k dc} = y_{s_k dc} - y_{s_k d}$. Combining equalities we obtain $x_d - x_{dc} = x_{s_{k-1} s_k d} - x_{s_{k-1} s_k dc}$. Continuing in this fashion we obtain

$$x_d - x_{dc} = x_{s_1 s_2 \dots s_k d} - x_{s_1 s_2 \dots s_k dc} = x_{dc} - x_{dc^2}$$

[1]We may assume without loss of generality that S contains the identity, since the player can pretend a certain permutation $t \in S$ happens every turn by default and then is followed by a permutation from the set $t^{-1} \cdot S$, which contains the identity.

and repeating the argument we have

$$x_d - x_{dc} = x_{dc} - x_{dc^2} = \cdots = x_{dc^{p-1}} - x_d$$

which holds for any $d \in G$. Notice that these p expressions sum to 0, so since p and q are distinct each expression must equal 0 and so the configuration $(x_1, x_2, \ldots, x_n)$ must have been semi-homogenous to begin with.

Therefore if the starting configuration is not semi-homogenous, the player can never force the configuration to be semi-homogenous and so cannot win. ■

Now we proceed to the second part of the proof of Theorem 6.1:

Lemma 6.3. The player can win the (G, m)-game if $(|G|, m) = (p^a, p)$ for some prime p and $a \in \mathbb{N}$.

Proof. We mimic the proof of Lemma 4.1. Suppose there exist vectors $x_0, x_1, \ldots, x_{n-1}$ that form a basis for $\mathbb{Z}_p^n$ and that have the property that $x_j - g \cdot x_j$ can be written as a linear combination of $x_1, x_2, \ldots, x_{j-1}$ for all $j \in \{0, 1, \ldots, n-1\}$ and all $g \in G$, where $g \cdot x$ represents the permutation of the coordinates of x corresponding to $g \in S_n$. For all $i \in \{1, 2, \ldots, p^n - 1\}$, let $y_i = x_{v_p(i)}$ where v_p denotes p-adic valuation. Then by the same reasoning as from the proof of Lemma 4.1, the sequence of moves $y_1, y_2, \ldots, y_{p^n-1}$ wins.

Thus it suffices to show that such a basis $x_0, x_1, \ldots, x_{n-1}$ exists. Consider the orbits of G on $\mathbb{Z}_p^n$, and suppose we partition $\mathbb{Z}_p^n$ into these orbits. Since $|G| = p^a$, the Orbit-Stabilizer Theorem implies that each orbit has size p^k for some $k \in \{0, 1, 2, \ldots, a\}$. Since the number of vectors in $\mathbb{Z}_p^n$ is p^n, the number of orbits of size 1 must be divisible by p. But note that 0 has an orbit of size 1, so there exists some nonzero $x_0 \in \mathbb{Z}_p^n$ fixed by G.

We can repeat the argument on the quotient space $\mathbb{Z}_p^n/\langle x_0 \rangle$ to find some nonzero $x_1 \in \mathbb{Z}_p^n/\langle x_0 \rangle$ that is fixed by G. Continuing in this fashion we obtain a nested sequence of subspaces

$$\langle x_0 \rangle < \langle x_0, x_1 \rangle < \cdots < \langle x_0, x_1, \ldots, x_{n-1} \rangle$$

each of which is fixed by G, and it is clear that the basis $x_0, x_1, \ldots, x_{n-1}$ satisfies the desired condition. This completes the proof. ■

Given a sequence of moves that wins the (G, p)-game, we can then induct on b as in Section 5 to construct a sequence of moves that wins the (G, p^b)-game for any $b \in \mathbb{N}$. Furthermore, if the player can win the (G, m)-game then since $S \subseteq G$ he can use the same sequence of moves to win the (S, m)-game, so the combination of Lemmas 6.2 and 6.3 imply Theorem 6.1, as desired. ■

7 Acknowledgements

The author would like to thank Dhroova Aiylam and Alexander Katz for their helpful discussion.