Setup:
- Standard die: 1, 2, 3, 4, 5, 6
- Sircherman die: 1, 2, 3, 4, 5, 6

Generating function perspective:
- Standard: \((x + x^2 + x^3 + x^4 + x^5 + x^6)^2\)
  
  Coeff of \(x^n\) is \# ways to get total sum \(n\) from roll of standard die.

- Sircherman die: \((x + 2x^2 + 2x^3 + x^4)(x + x^3 + x^4 + x^5 + x^6 + x^8)\)

Starting from scratch: how to find this new factorization?
- Is there no other solutions?

Few observations: generating function for a labeling of a die has
- sum of coeffs equal to 6
- coeffs are non-negative integers.
- no constant term

Goal: Find all pairs \(p(x), q(x)\) satisfying these conditions &
\[ p(x)q(x) = (x + \ldots + x^6)^2 \]
\[ x + x^2 + x^3 + x^4 + x^5 + x^6 = x(1 + \ldots + x^5) = x \cdot \frac{x^6 - 1}{x - 1} = x \cdot \Phi_6(x) \Phi_3(x) \Phi_2(x) \]

Facts: 
1. \(\Phi_d(x)\) always has integer coefficients
2. \(\Phi_d(x)\) is irreducible as polynomial w/ integer coeff.

\[ p(x)q(x) = x \cdot \Phi_6(x) \cdot \Phi_6(x) \cdot \Phi_3(x) \cdot \Phi_3(x) \cdot \Phi_2(x) \cdot \Phi_2(x) \]

Select some to contribute to \(p\), rest contribute to \(q\).
\[ p: x \quad \exists_2 \quad \exists_3 \]
\[ q: x \quad \exists_2 \quad \exists_3 \quad \exists_4 \quad \exists_5 \]

\[ \sum \text{of cost} \]
\[ \exists_2(x) = x + 1 \quad 2 \]
\[ \exists_3(y) = x^2 + x + 1 \quad 3 \]
\[ \exists_5(y) = x^2 - x + 1 \quad 1 \]

100 prisoners problem

Setup: 100 boxes, each one with name (each appearing exactly once).

Each prisoner can independently go and check 50 boxes.

Goal: each person needs to find their name.

Naively: each person open 50 boxes at random.

success rate: \((\frac{1}{2})^{100}\)

Slightly better: alternate between opening first 50 & second 50.

If first gets it right: \(\frac{1}{2}\), \(\rightarrow\) \(\frac{25}{99}\)

For second to get it right: \(\frac{50}{99}\).

assuming first got it right.

Success rate is \((\frac{25}{99})^{50}\) > \((\frac{25}{100})^{50}\)

Better strategy: assign \(1...100\) to each prisoner.

Strategy: each person opens their number.

if not their name, go to whatever box corresponds to name they find. Repeat.
Math version: setup of new is permutation of \( C(100, j) \).

we win if for all \( i \), the sequence

\( f(i), f^2(i), \ldots, f^{50}(i) \) contains \( i \).

How many permutations have this property?

i.e., how many do not contain cycle of length \( \geq 51 \).

Complement: how many have cycle of length \( \geq 51 \)?

Suppose we have cycle of length \( r \), \( r \geq 51 \).

Then this cycle is unique: how many?

\[
\sum_{r=51}^{100} \binom{100}{r} \frac{(100)!}{(100-r)!} = \sum_{r=51}^{100} \frac{100!}{r!(100-r)!} = \sum_{r=51}^{100} \frac{100!}{r}
\]

Probability of success is

\[1 - \sum_{r=51}^{100} \frac{1}{r} \approx 0.3\]

General case: permutation of size \( 2n \)

How many do not have cycle of length \( \geq n+1 \)?

\[1 - \sum_{r=n+1}^{2n} \frac{1}{r}\]

Euler's constant: \( \exists \gamma \) such that

\[
\lim_{n \to \infty} \left( \sum_{r=1}^{n} \frac{1}{r} - \log(n) \right) = \gamma
\]
\[
\lim_{n \to \infty} \left( 1 - \sum_{r=1}^{\infty} \frac{1}{r} \right) = \lim_{n \to \infty} \left( 1 - \sum_{r=1}^{\infty} \frac{1}{r} + \sum_{r=1}^{n} \frac{1}{r} \right)
\]
\[
= \lim_{n \to \infty} \left( 1 - \sum_{r=1}^{\infty} \frac{1}{r} + \log(2n) - \log(2n) + \sum_{r=1}^{n} \frac{1}{r} - \log(n) + \log(n) \right)
\]
\[
= \lim_{n \to \infty} \left( 1 - \log(2n) + \log n \right) = \lim_{n \to \infty} \left( 1 - \log 2 \right)
\]
\[
\approx 1 - \log 2 \approx 0.30685...
\]

Variant: unlabeled boxes, labeled 1, ..., n.
Each one contains key to a box you pick them all at one.
You may destroy k boxes initially. (Key survives)
Chance you get to open all boxes?

Fix k, prove by induction on n.
We may as well pick first k boxes.
Permutation version: what is chance that a random permutation of \([n]\), every cycle contains at least one of \(1, \ldots, k\)?
(all these "good"

Prove by induction on n that \(\#\) of such permutations
\[
is \frac{k}{n} \cdot n! = k(n-1)!
\]

Base case: \(n=k\). All permutations have this property

Induction step: \(n=k\), count is valid for \(n-1\).
\(n\) cannot be in its own cycle.
I can remove \(n\) from this permutation to get
a permutation of size $n-1$ with desired properties
and I can recover my permutation if I remember which
number it followed (i.e., which $i$ satisfies $f(i) = n$)

\[
\# \text{good permutations} = \frac{\# \text{good permutation}}{(n-1)} \times (n-1) = k(n-2)! \times (n-1) = k(n-1)!
\]

Odd-town. Odd-town has $n$ people living in it.

- They like to form clubs. Rules:
  1. Each club has odd # of members.
  2. Any 2 clubs have even size overlap.

\[ \Rightarrow \text{Thm. There are } S_n \text{ clubs.} \]

- Setup. Linear algebra can be done w/ scalars being any field.
  - can add, subtract, multiply, divide by nonzero.

Finite fields: $\mathbb{Z}/p$ integers modulo $p$ where $p$ is prime.

More specifically, $\mathbb{Z}/2 = \{ 0, 1 \}$

\[
\begin{align*}
\mathbb{F}_2 & \quad \text{even} \quad \text{odd} \\
0 & \quad 0 \\
1 & \quad 1
\end{align*}
\]

Translation. Vector space $\mathbb{F}_2^n = \{ (a_1, \ldots, a_n) \mid a_i \in \mathbb{F}_2 \}$

- club = subset of $C_{\mathbb{F}_2 \times}$ = vector in $(\mathbb{F}_2)^n$

\[ S \rightarrow (a_1, \ldots, a_n) \text{ where } a_i = 1 \text{ if } i \in S, a_i = 0 \text{ if } i \notin S. \]

\[ a_S \]
dot product: \((a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = a_1 b_1 + \cdots + a_n b_n\)

Note: \(a_i b_i = 1 \text{ if } i \in \text{both clubs} \),
\(0 \text{ otherwise}\).

\(X_s \cdot X_T = \begin{cases} 1 & \text{if } |T| \text{ odd} \\ 0 & \text{if } |T| \text{ even} \end{cases} \)

Claim: If clubs \(S_1, \ldots, S_r\) satisfy 2 rules, then \(X_{S_1}, \ldots, X_{S_r}\) are linearly independent.

Suppose we have linear dependence:

\[c_1 X_{S_1} + c_2 X_{S_2} + \cdots + c_r X_{S_r} = 0 \quad c_i \in \mathbb{F}_2.\]

Take dot product with \(X_{S_i}\):

\[c_1 (X_{S_i} \cdot X_{S_1}) + c_2 (X_{S_i} \cdot X_{S_2}) + \cdots + c_r (X_{S_i} \cdot X_{S_r}) = 0 \cdot X_{S_i} = 0.\]

By (2), \(X_{S_j} \cdot X_{S_i} = 0 \text{ if } i \neq j\).

By (1), \(X_{S_i} \cdot X_{S_i} = 1\)

\[c_i = 0.\]

True for any \(i\), so \(X_{S_1}, \ldots, X_{S_r}\) linearly independent.

\[\dim(\mathbb{F}_2^n) \leq n \implies r \leq n.\]