Setup: standard dice 1, 2, 3, 4, 5, 6
1, 2, 3, 4, 5, 6

Sicherman dice: 1, 2, 2, 3, 3, 4
1, 3, 4, 5, 6, 8

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 dice.

Sicherman dice: $(x+2x^2+2x^3+x^4)(x+x^3+x^4+x^5+x^6+x^8)$

starting from scratch: how to find this new factorization?
Show no other solutions?

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

Goal: Find all pairs $p(x)$, $q(x)$ satisfying these conditions
& $p(x)q(x) = (x+\dots+x^6)^2$

$$x+x^2+x^3+x^4+x^5+x^6 = x(1+\dots+x^5) = x\cdot\frac{x^6-1}{x-1}.$$

$$= x\,\Phi_6(x)\,\Phi_3(x)\,\Phi_2(x)$$

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

$$p(x)q(x) = \underline{x}\cdot\underline{x}\cdot\Phi_6(x)\cdot\Phi_6(x)\cdot\Phi_3(x)\cdot\Phi_3(x)\cdot\Phi_2(x)\cdot\Phi_2(x)$$

select some to contribute to p, rest contribute to q.

p: $\quad x \quad \Phi_2 \quad \Phi_3$

q: $\quad x \quad \Phi_2 \quad \Phi_3 \quad \Phi_6 \quad \Phi_6$

	sum of coeff
$\Phi_2(x) = x+1$	2
$\Phi_3(x) = x^2+x+1$	3
$\Phi_6(x) = x^2-x+1$	1

---

100 prisoners problem

Setup: 100 boxes, each one w/ name (each appearing exactly once)

100 prisoners

Each prisoner can independently go and check 50 boxes.

Goal: each person needs to find their name.

Naively: each person opens 50 boxes at random.

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

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

if first gets it right: $\frac{1}{2}$. $\quad \rightarrow \quad \frac{25}{99}$

for second to get it right assuming first got it right $50/99$.

success rate is $\left(\frac{25}{99}\right)^{50} > \left(\frac{25}{100}\right)^{50}$

better strategy: assign #s 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 names is permutation f of $[100]$.

we win if for all i, the sequence

$$f(i), f^2(i), \ldots, f^{50}(i) \quad \text{contains } i$$

How many permutations have this property?

ie, how many do not contain cycle of length ≥ 51

Complement: how many have cycle of length ≥ 51?

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

Then this cycle is unique: how many?

$$\sum_{r=51}^{100} \binom{100}{r} (r-1)!\,(100-r)! = \sum_{r=51}^{100} \frac{100!}{r!\,\cancel{(100-r)!}} (r-1)!\,\cancel{(100-r)!} = \sum_{r=51}^{100} \frac{100!}{r}$$

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: $\exists\, \gamma$ s.t.

$$\lim_{n\to\infty} \left(\sum_{r=1}^{n} \frac{1}{r} - \log(n) \right) = \gamma$$

$$\lim_{n\to\infty}\left(1-\sum_{r=n+1}^{2n}\frac{1}{r}\right) = \lim_{n\to\infty}\left(1-\sum_{r=1}^{2n}\frac{1}{r}+\sum_{r=1}^{n}\frac{1}{r}\right)$$

$$= \lim_{n\to\infty}\Big(1-\underbrace{\sum_{r=1}^{2n}\frac{1}{r}+\log(2n)}_{-\gamma}-\log(2n)+\underbrace{\sum_{r=1}^{n}\frac{1}{r}-\log(n)}_{\gamma}+\log n\Big)$$

$$= \lim_{n\to\infty}(1-\log(2n)+\log n) = \lim_{n\to\infty}(1-\log 2)$$

$$= 1-\log(2) \approx 0.30685\ldots$$

Variant: n locked boxes, labeled $1,\ldots,n$.

each one contains key to a box / you pick them all at once

You may destroy k boxes initially. (key survives)

Chance you get to open all boxes? k/n

Fix k, prove by induction on n.

We may as well pick first k boxes.

Permutation version: what is chance that for a random permutation of $[n]$, every cycle contains at least one of $1,\ldots,k$?

call 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 $\to n!$ ✓

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 $n-1$ w/ desired properties and I can recover my permutation if I remember what number it followed (i.e., which i satisfies $f(i)=n$)

$$\boxed{\#\text{ good permutations of } n = \#\text{ good permutations of } n-1 \cdot (n-1)}$$

$$= k(n-2)! \cdot (n-1) = k(n-1)!$$

$\square$

<u>Oddtown.</u> Oddtown 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.

$\Rightarrow$ <u>Thm.</u> There are $\leq n$ clubs.

<u>Setup.</u> Linear algebra can be done w/ scalars being any <u>field</u>.

can add, subtract, multiply, divide by nonzero.

<u>Finite fields:</u> $\mathbb{Z}/p$ integers modulo $p \leftarrow$ prime.

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

$\mathbb{Z}/2 = \mathbb{F}_2$, $0 \leftarrow$ even, $1 \leftarrow$ odd

<u>Translation.</u> Vector space $(\mathbb{F}_2)^n = \{(a_1, \dots, a_n) \mid a_i \in \mathbb{F}_2\}$

club = subset of $[n]$ = vector in $(\mathbb{F}_2)^n$

$S \to \underbrace{(a_1, \dots a_n)}_{= \chi_S}$ where $a_i = \begin{cases} 1 & \text{if } i \in S \\ 0 & \text{if } i \notin S \end{cases}$

dot product: $(a_1, \dots, a_n) \cdot (b_1, \dots b_n) = a_1 b_1 + \dots + a_n b_n$

Note: $a_i b_i = 1$ if $i \in$ both clubs
$\quad\quad 0$ else

$$\chi_S \cdot \chi_T = \begin{cases} 1 & \text{if } |S \cap T| \text{ odd} \\ 0 & \text{if } |S \cap T| \text{ even} \end{cases}$$

Claim: If clubs $S_1, \dots S_r$ satisfy 2 rules then $\chi_{S_1}, \dots, \chi_{S_r}$ are linearly independent.

suppose we have linear dependence:

$$c_1 \chi_{S_1} + c_2 \chi_{S_2} + \dots + c_r \chi_{S_r} = 0 \quad c_i \in \mathbb{F}_2.$$

Take dot product w/ χ_{S_i}.

$$c_1 \chi_{S_1} \cdot \chi_{S_i} + c_2 \chi_{S_2} \cdot \chi_{S_i} + \dots + c_r \chi_{S_r} \cdot \chi_{S_i} = 0 \cdot \chi_{S_i} = 0.$$

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

By (1), $\chi_{S_i} \cdot \chi_{S_i} = 1$

$$c_i = 0$$

True for any i, so $\chi_{S_1}, \dots \chi_{S_r}$ linearly independent.

$\dim (\mathbb{F}_2)^n \leq n \Rightarrow r \leq n.$ $\square$