# The Probabilistic Method

## Week 5: Linearity Of Expectation

Joshua Brody
CS49/Math59
Fall 2015

# Clicker Question

Let **P** be the uniform distribution on **$\Omega$={0,1,2,3,4,5,6,7}**. Which of the following random variables are **not** uniform on **S={0,1,2,3,4,5,6,7}**?

(A) **$X_1$(w) := w + 2 (mod 8)**

(B) **$X_2$(w) := w + 5 (mod 8)**

(C) **$Y_1$(w) := 2w (mod 8)**

(D) **$Y_2$(w) := 3w (mod 8)**

(E) **None of the above *(all are uniform on S)***

# Clicker Question

Let **P** be the uniform distribution on **Ω={0,1,2,3,4,5,6,7}**. Which of the following random variables are **not** uniform on **S={0,1,2,3,4,5,6,7}**?

(A) **$X_1(w) := w + 2 \pmod 8$**

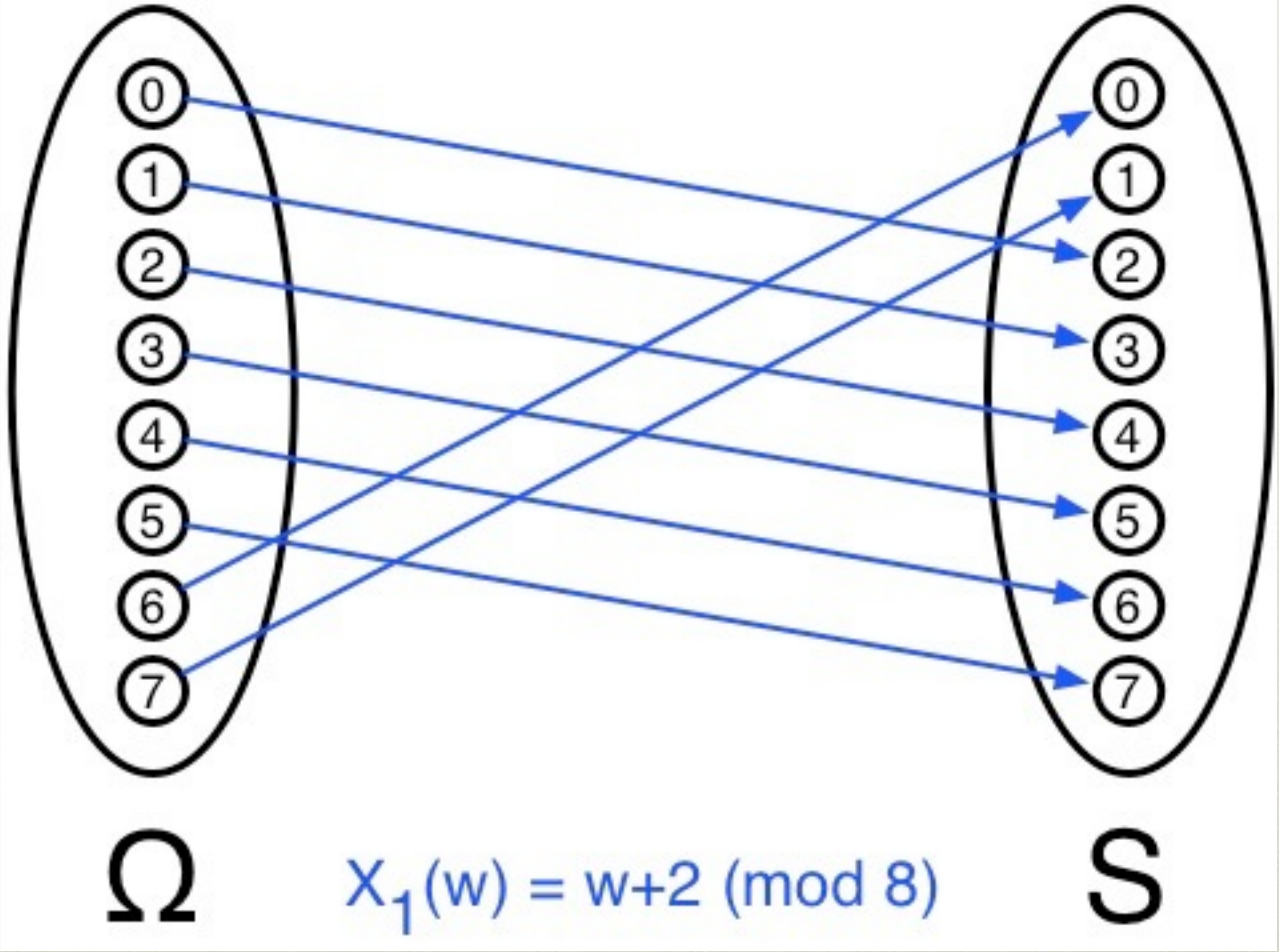
(B) **$X_2(w) := w + 5 \pmod 8$**

(C) **$Y_1(w) := 2w \pmod 8$**

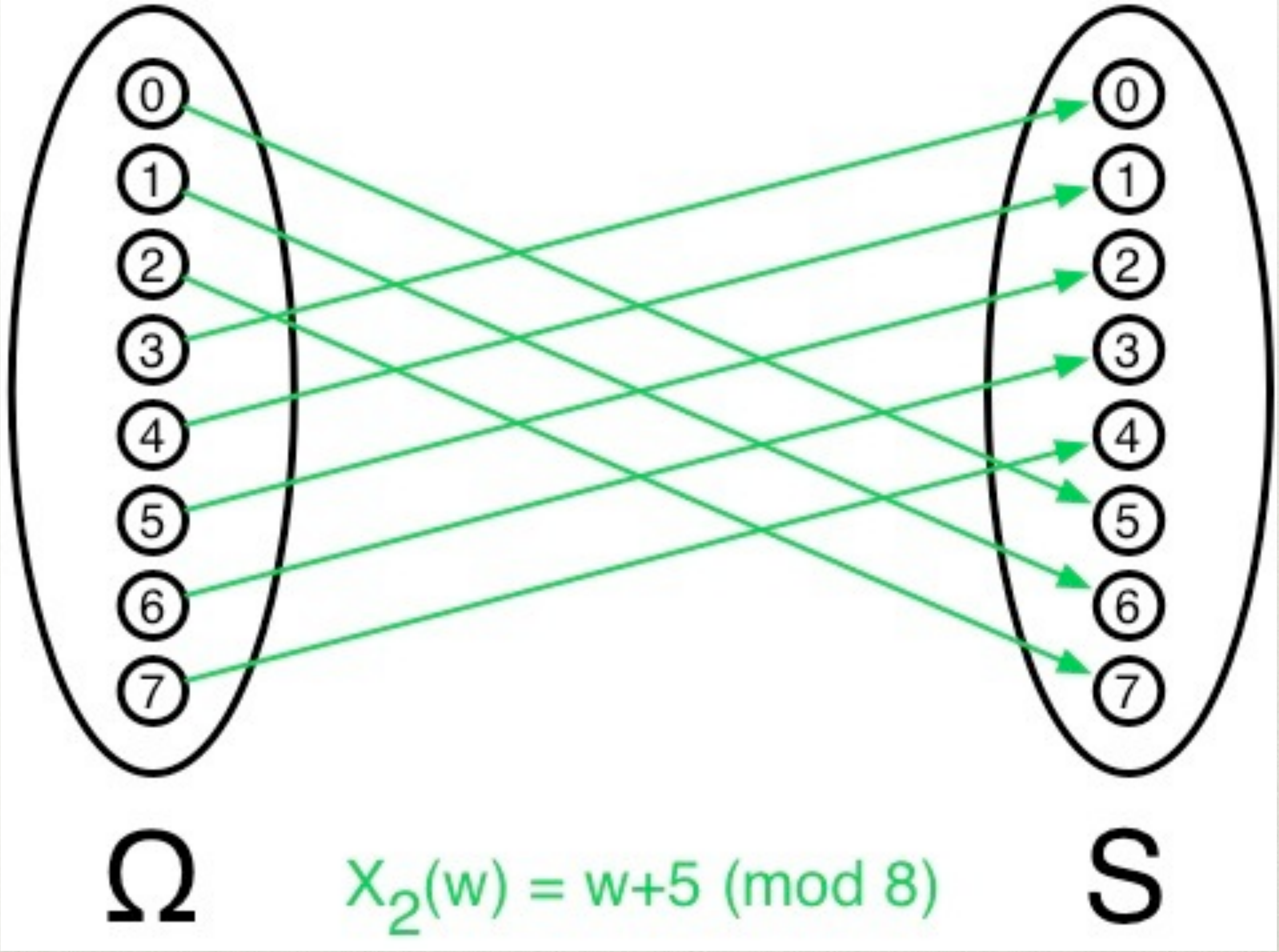
(D) **$Y_2(w) := 3w \pmod 8$**

(E) **None of the above *(all are uniform on S)***

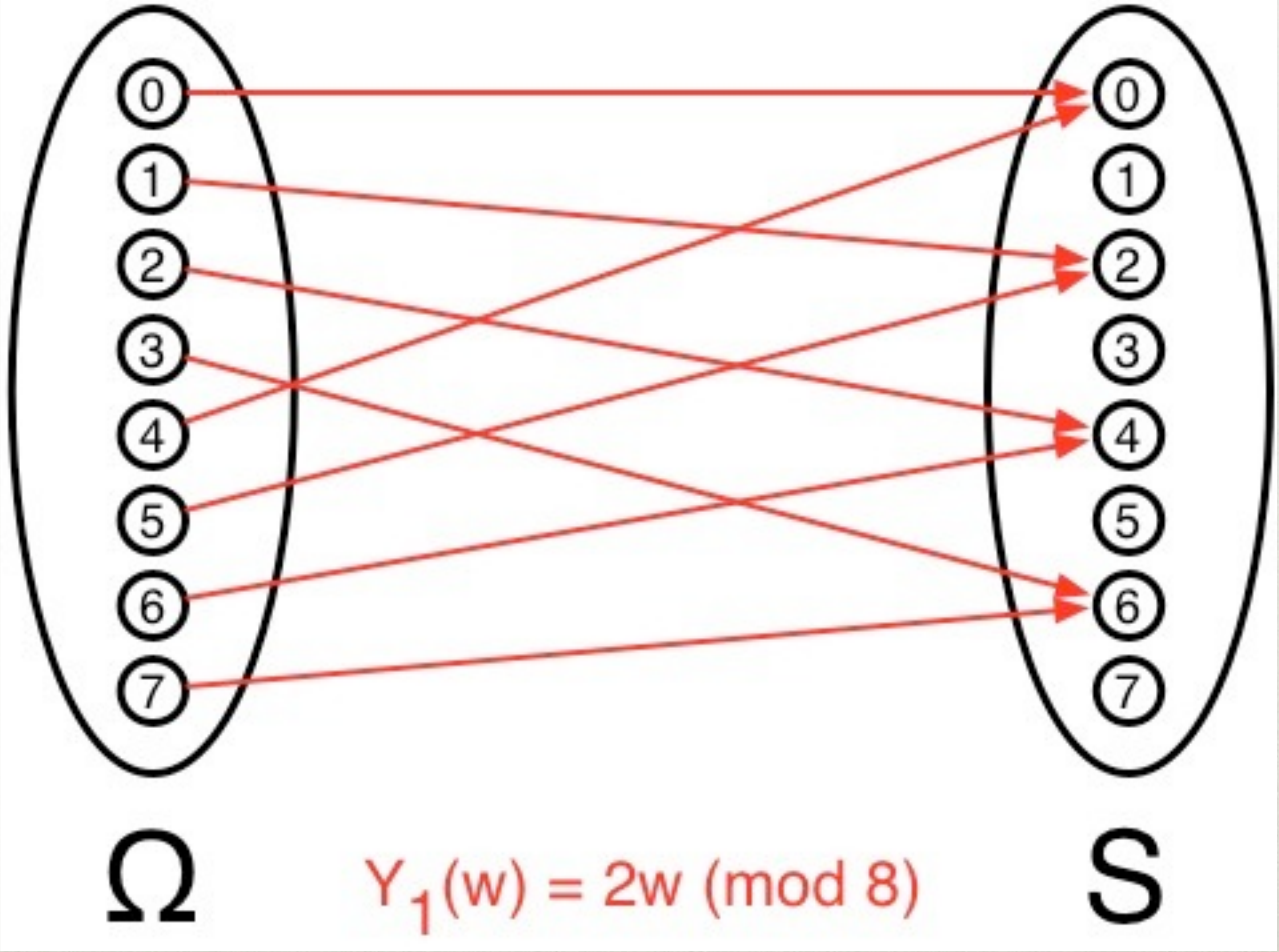
# Uniform Random Variables



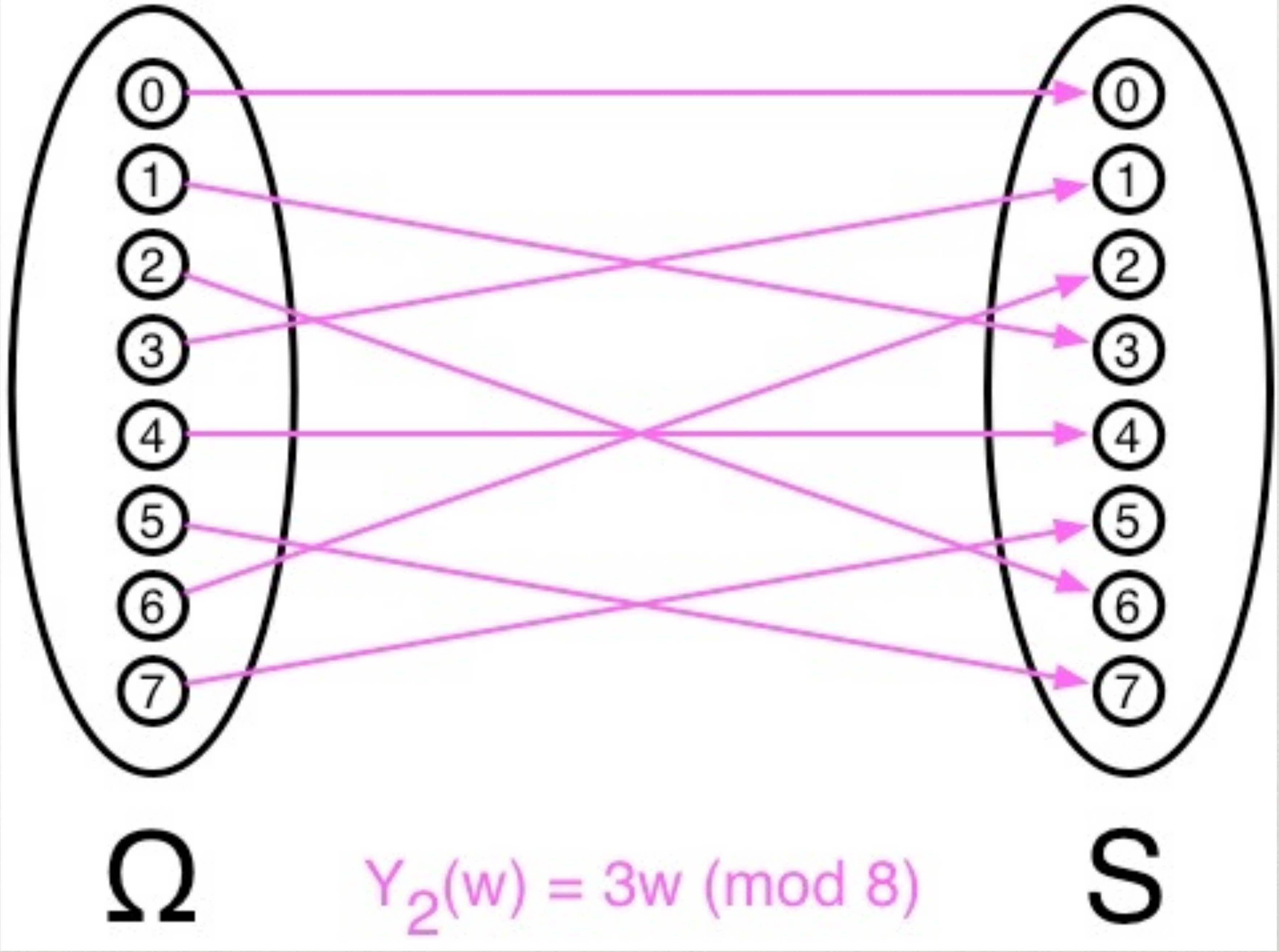
# Uniform Random Variables



# Uniform Random Variables



# Uniform Random Variables



# Sum-Free Sets

A set of integers **A** is **sum-free** if there are no elements $\mathbf{a_1, a_2, a_3} \in \mathbf{A}$ such that $\mathbf{a_1 + a_2 = a_3}$.

sum-free:

**{1, 3, 8, 10, 12}** **{11, 15, 19, 23, 31}**

not sum-free:

**{1, 2, 4, 6, 11}** **{0, 14, 139, 150, 200}**

# Sum-Free Sets

**Theorem:** every set **B** of **n** nonzero integers has a sum-free subset **A** of size **> n/3.**

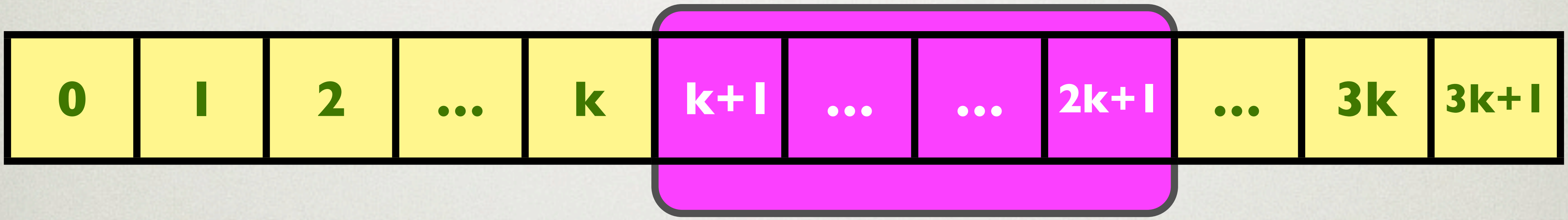
**example:** integers **mod m,** **(m = 3k+2)**

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | … | k | k+1 | … | … | 2k+1 | … | 3k | 3k+1 |

# Sum-Free Sets

**Theorem:** every set **B** of **n** nonzero integers has a sum-free subset **A** of size **> n/3.**

**example:** integers **mod m,** **(m = 3k+2)**

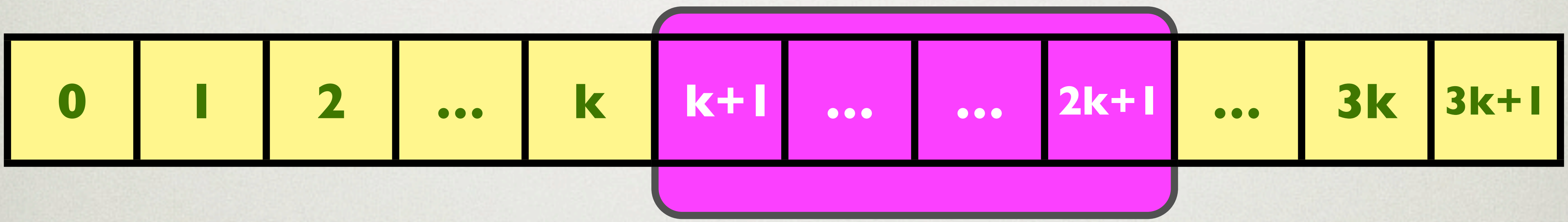



**C = {k+1, ..., 2k+1}**

# Sum-Free Sets

**Theorem:** every set **B** of **n** nonzero integers has a sum-free subset **A** of size **> n/3.**

**example:** integers **mod m,** **(m = 3k+2)**




**C = {k+1, ..., 2k+1}**

- $a_1 = (k+1) + i$
- $a_2 = (k+1) + j$

# Sum-Free Sets

**Theorem:** every set **B** of **n** nonzero integers has a sum-free subset **A** of size **> n/3.**

**example:** integers **mod m,** **(m = 3k+2)**

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | … | k | k+1 | … | … | 2k+1 | … | 3k | 3k+1 |

**C = {k+1, …, 2k+1}**

- $a_1 = (k+1) + i$
- $a_2 = (k+1) + j$
- $a_1 + a_2 \geq 2k+2, \quad a_1 + a_2 \leq 4k+2 \equiv k \pmod{3k+2}$

# First Attempt

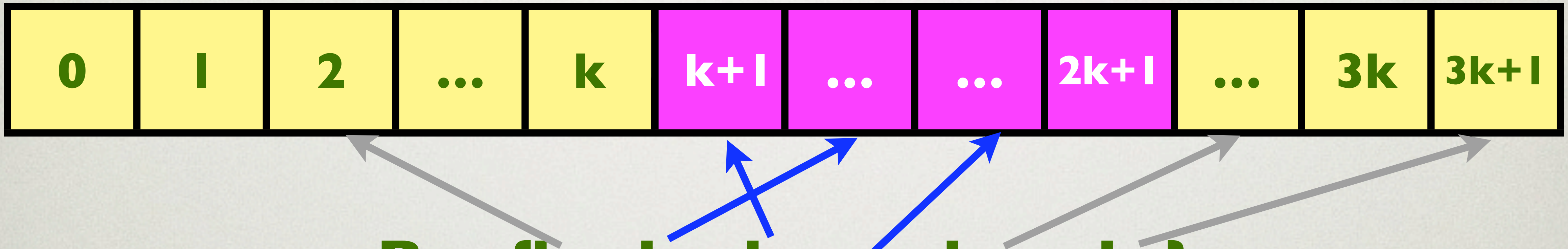
**Theorem:** every set **B** of **n** nonzero integers has a sum-free subset **A** of size **> n/3.**

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | … | k | k+1 | … | … | 2k+1 | … | 3k | 3k+1 |

$$B = \{b_1, b_2, b_3, \dots, b_{n-1}, b_n\}$$

# First Attempt

**Theorem:** every set **B** of **n** nonzero integers has a sum-free subset **A** of size **> n/3.**

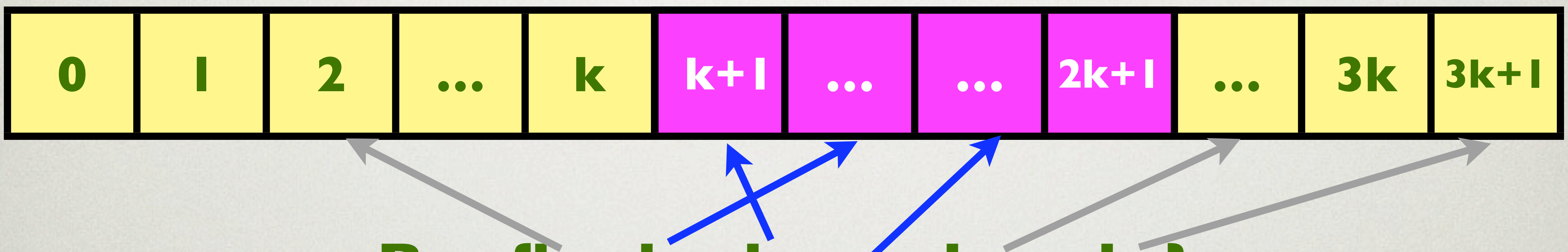



$B = \{b_1, b_2, b_3, \ldots, b_{n-1}, b_n\}$

$A = \{b_i \in B : b_i \pmod{m}$ is in $C\}$

# First Attempt

**Theorem:** every set **B** of **n** nonzero integers has a sum-free subset **A** of size **> n/3.**




$B = \{b_1, b_2, b_3, \ldots, b_{n-1}, b_n\}$

$A = \{b_i \in B : b_i \pmod{m}$ is in $C\}$

- good news: **A** is sum-free!

# Clicker Question

**$C = \{k+1, \ldots, 2k+1\}$**

**$A = \{b_i \in B : b_i \pmod{m}$ is in $C\}$.**

What is **$|A|$**?

(A) **$|A| = n/3$**

(B) **$|A| = (k+1)/(3k+2)$**

(C) **$|A| > n/2$**

(D) **$|A| = 0$**

(E) **Multiple answers possible**

# Clicker Question

$C = \{k+1, \ldots, 2k+1\}$

$A = \{b_i \in B : b_i \pmod{m}$ is in $C\}$.

What is $|A|$?

(A) $|A| = n/3$

(B) $|A| = (k+1)/(3k+2)$

(C) $|A| > n/2$

(D) $|A| = 0$

(E) Multiple answers possible

# First Attempt

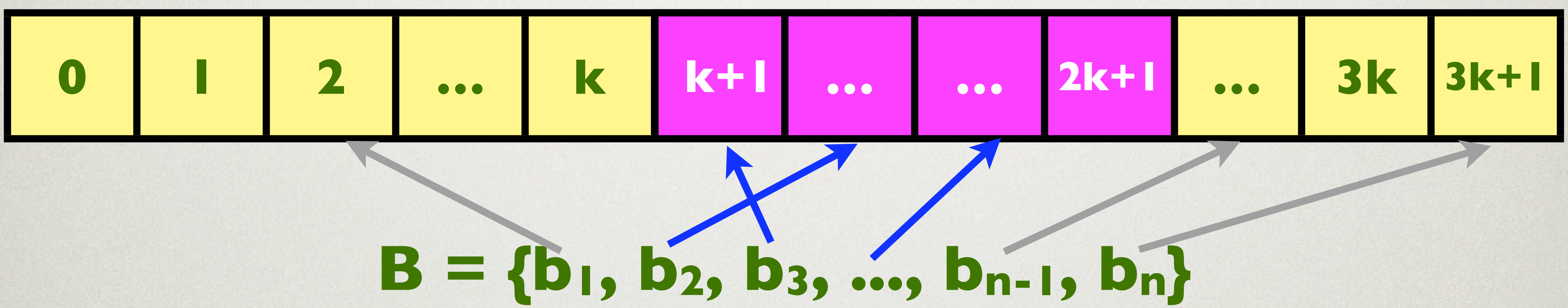
**Theorem:** every set **B** of **n** nonzero integers has a sum-free subset **A** of size **> n/3.**

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | ... | k | k+1 | ... | ... | 2k+1 | ... | 3k | 3k+1 |

$$B = \{b_1, b_2, b_3, \ldots, b_{n-1}, b_n\}$$

# First Attempt

**Theorem:** every set **B** of **n** nonzero integers has a sum-free subset **A** of size **> n/3.**

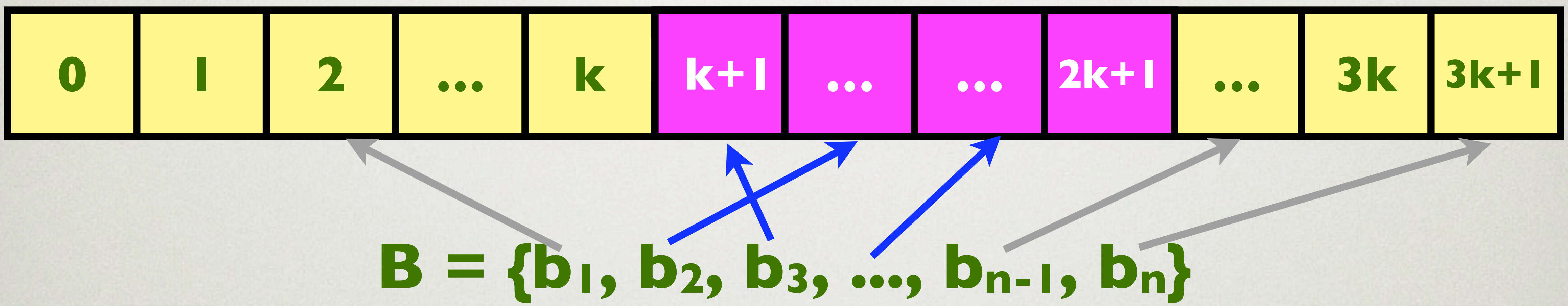



$A = \{b_i \in B : b_i \pmod{m}$ is in $C\}$

- good news: **A** is sum-free!

# First Attempt

**Theorem:** every set **B** of **n** nonzero integers has a sum-free subset **A** of size **> n/3.**




**$A = \{b_i \in B : b_i \pmod{m}$** is in **C}**

- good news: **A** is sum-free!
- bad news: maybe **|A| = 0** (ex. **B={m,2m,3m,...}**)

# SECOND ATTEMPT

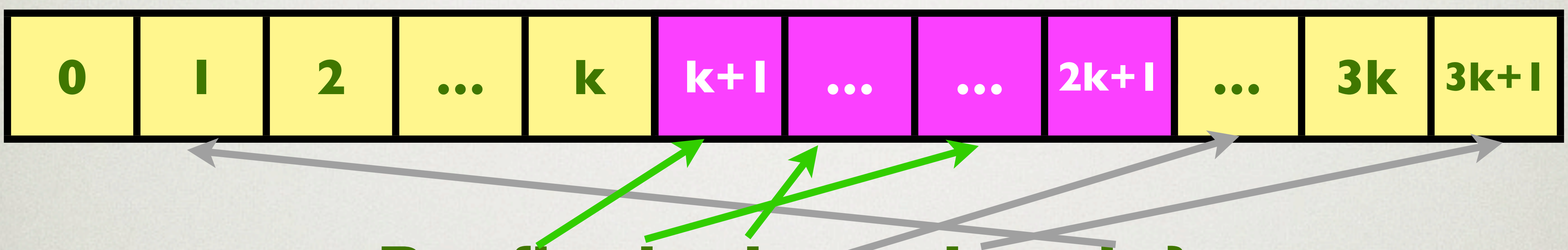
**idea:** shift by random $\mathbf{0 \le R < m}$

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | ... | k | k+1 | ... | ... | 2k+1 | ... | 3k | 3k+1 |

$$\mathbf{B = \{b_1, b_2, b_3, \ldots, b_{n-1}, b_n\}}$$

# SECOND ATTEMPT

**idea:** shift by random $0 \leq R < m$

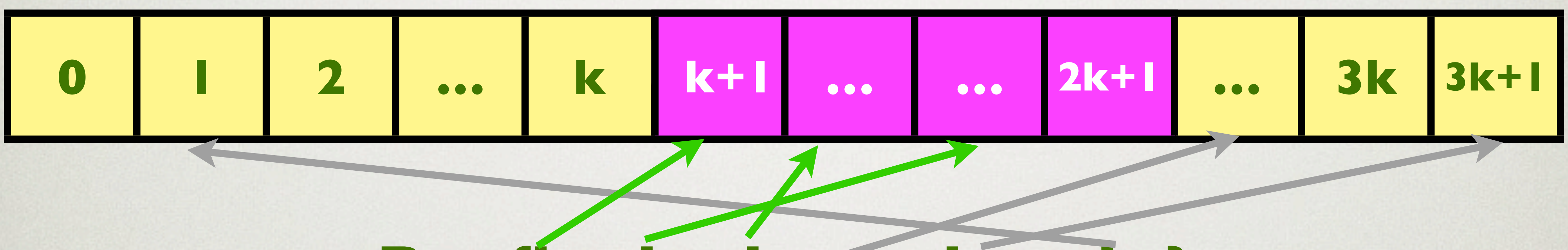



$B = \{b_1, b_2, b_3, \ldots, b_{n-1}, b_n\}$

$A = \{b_i \in B : b_i + R \pmod{m}$ is in $C\}$

# SECOND ATTEMPT

**idea:** shift by random $0 \leq R < m$



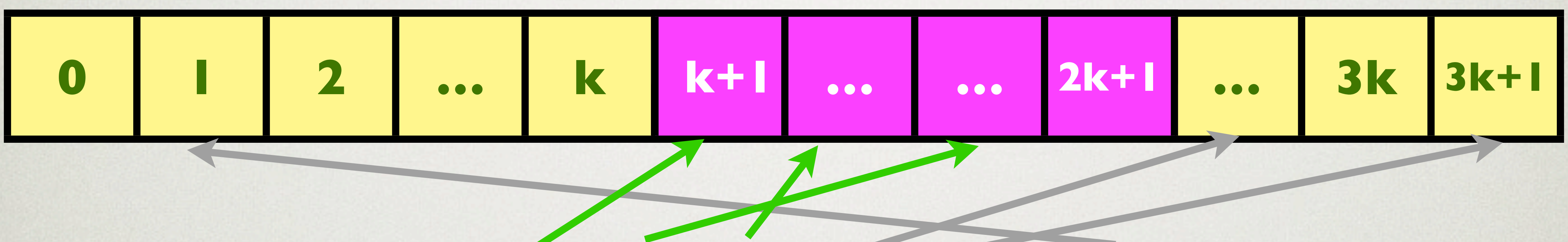

$B = \{b_1, b_2, b_3, \ldots, b_{n-1}, b_n\}$

$A = \{b_i \in B : b_i + R \pmod{m}$ is in $C\}$

- good news: $E[|A|] > n/3$

# SECOND ATTEMPT

**idea:** shift by random $0 \le R < m$




$B = \{b_1, b_2, b_3, \ldots, b_{n-1}, b_n\}$

$A = \{b_i \in B : b_i + R \pmod{m}$ is in $C\}$

- good news: $E[|A|] > n/3$
- bad news: **A** not always sum-free

# Third Attempt

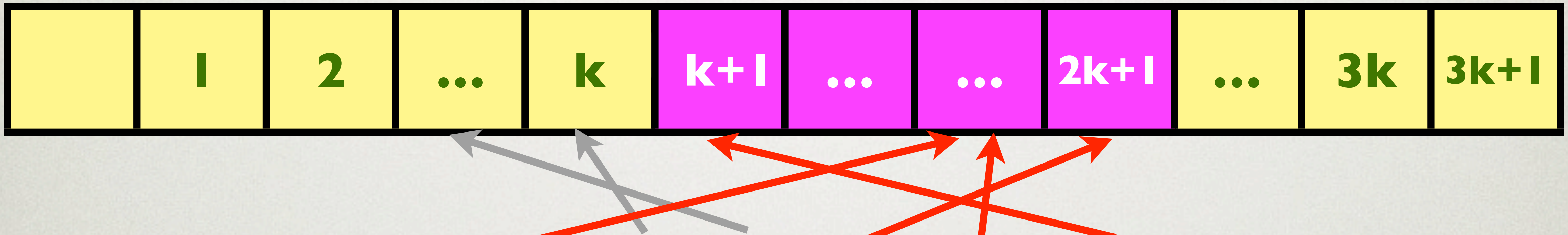
**idea:** multiply by random $1 \leq R < m$

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | ... | k | k+1 | ... | ... | 2k+1 | ... | 3k | 3k+1 |

$$B = \{b_1, b_2, b_3, \ldots, b_{n-1}, b_n\}$$

# Third Attempt

**idea:** multiply by random $1 \leq R < m$

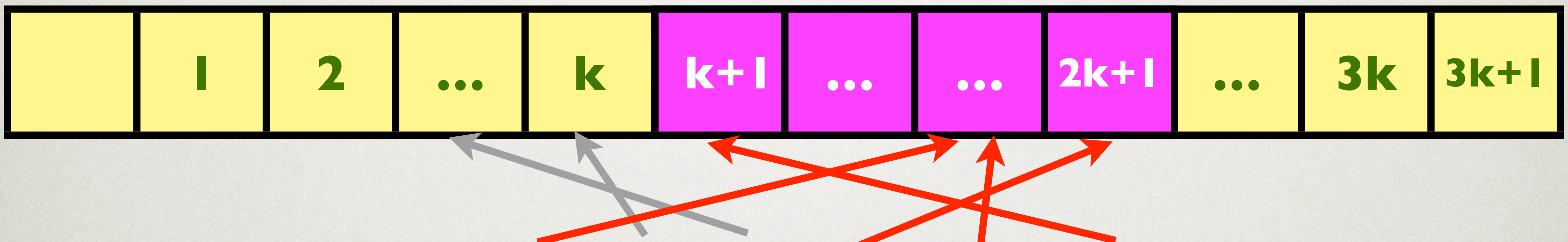



$B = \{b_1, b_2, b_3, ..., b_{n-1}, b_n\}$

$A = \{b_i \in B : b_i * R \pmod{m}$ is in $C\}$

# Third Attempt

**idea:** multiply by random $1 \leq R < m$



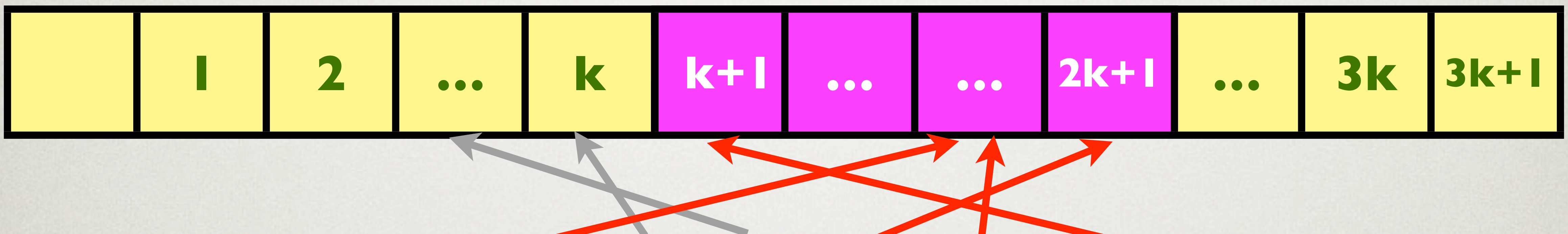

$B = \{b_1, b_2, b_3, ..., b_{n-1}, b_n\}$

$A = \{b_i \in B : b_i{*}R \pmod m$ is in $C\}$

- good news: $E[|A|] > n/3$

# Third Attempt

**idea:** multiply by random $1 \leq R < m$




$B = \{b_1, b_2, b_3, ..., b_{n-1}, b_n\}$

$A = \{b_i \in B : b_i * R \pmod{m}$ is in $C\}$

- good news: $E[|A|] > n/3$
- more good news: **A** sum-free!

# Solution

**Theorem:** every set **B** of **n** nonzero integers has a sum-free subset **A** of size **> n/3.**

**proof:**

- pick large prime $p = 3k+2$ s.t. $p > 2\max|b_i|$
- sample uniform element $R \in \{1, \ldots, p-1\}$
- $C := \{k+1, \ldots, 2k+1\}$
- $A := \{b_i : b_i * R \pmod{p} \in C\}$
- **Fact 1:** $E[|A|] > n/3$
- **Fact 2:** **A** is sum-free.

# The Probabilistic Method