# Random Multiplicative Walks on the Integers Modulo $n$

Nathan McNew
Towson University

Special Session on Analytic Number Theory and Arithmetic
Joint Mathematics Meetings
Atlanta, Georgia
January 7th, 2017

# Random walks

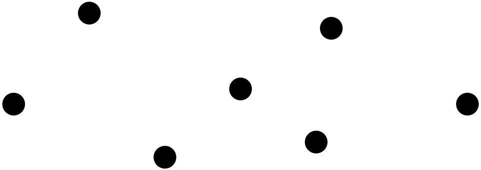
A **random walk** is a set of states and possible (weighted) transitions between them.

# Random walks

A **random walk** is a set of states and possible (weighted) transitions between them. Starting from an initial state $X_0$, each subsequent state is randomly chosen from the possible transitions from the prior state.

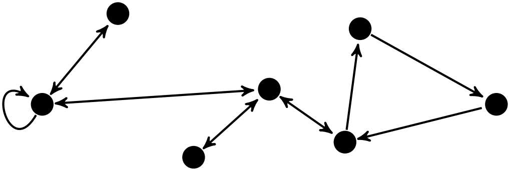
# Random walks

A **random walk** is a set of states and possible (weighted) transitions between them. Starting from an initial state $X_0$, each subsequent state is randomly chosen from the possible transitions from the prior state.



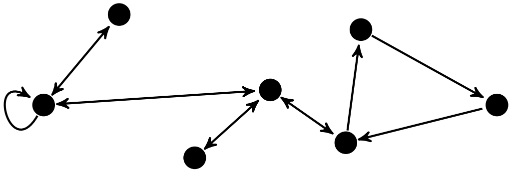
# Random walks

A **random walk** is a set of states and possible (weighted) transitions between them. Starting from an initial state $X_0$, each subsequent state is randomly chosen from the possible transitions from the prior state.



# Random walks

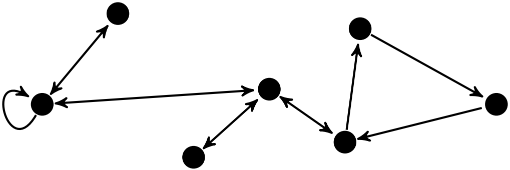
A **random walk** is a set of states and possible (weighted) transitions between them. Starting from an initial state $X_0$, each subsequent state is randomly chosen from the possible transitions from the prior state.



A random walk is **transitive** if it is possible to get from any one state to any other state in a finite number of steps.

# Random walks

A **random walk** is a set of states and possible (weighted) transitions between them. Starting from an initial state $X_0$, each subsequent state is randomly chosen from the possible transitions from the prior state.



A random walk is **transitive** if it is possible to get from any one state to any other state in a finite number of steps.

A state is **absorbing** if it is not possible to leave that state.

# Random walks on groups

# Random walks on groups

Make a random walk from a group, $G$:

# Random walks on groups

Make a random walk from a group, $G$:

Take the elements of $G$ to be the states of the random walk.

# Random walks on groups

Make a random walk from a group, $G$:

Take the elements of $G$ to be the states of the random walk.

Fix a generating set $S$ of the group.

# Random walks on groups

Make a random walk from a group, $G$:

Take the elements of $G$ to be the states of the random walk.

Fix a generating set $S$ of the group. Each step consists of acting on the current state by one of the elements of $S$ chosen at random.

# Random walks on groups

Make a random walk from a group, $G$:

Take the elements of $G$ to be the states of the random walk.

Fix a generating set $S$ of the group. Each step consists of acting on the current state by one of the elements of $S$ chosen at random.

Note that since the elements of $S$ generate $G$, this walk will be transitive, and there are no absorbing elements.

# Random walks on groups

# Random walks on groups

**Examples:**

# Random walks on groups

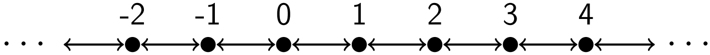
**Examples:**

$G = \mathbb{Z}$, $S = \{\pm 1\}$, $X_0 = 0$

# Random walks on groups

**Examples:**

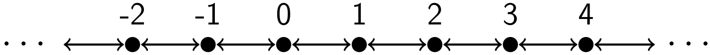
$G = \mathbb{Z}$, $S = \{\pm 1\}$, $X_0 = 0$



# Random walks on groups

**Examples:**

$G = \mathbb{Z}$, $S = \{\pm 1\}$, $X_0 = 0$

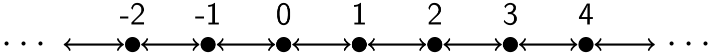



$G = \mathbb{Z}/n\mathbb{Z}$, $S = \{\pm 1\}$, $X_0 = 0$

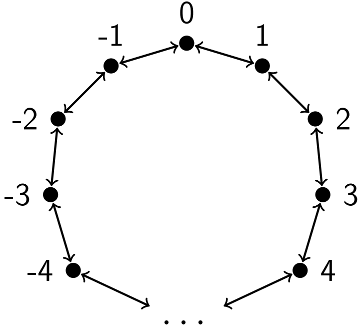
# Random walks on groups

**Examples:**

$G = \mathbb{Z}$, $S = \{\pm 1\}$, $X_0 = 0$




$G = \mathbb{Z}/n\mathbb{Z}$, $S = \{\pm 1\}$, $X_0 = 0$



# Random walks on monoids

Recently several authors (Gretete, Mairesse, . . . ) have generalized many of the ideas from random walks on groups to monoids.

# Random walks on monoids

Recently several authors (Gretete, Mairesse, . . . ) have generalized many of the ideas from random walks on groups to monoids.

Recall: A **monoid** is almost a group, but some elements may not have inverses.

# Random walks on monoids

Recently several authors (Gretete, Mairesse, . . . ) have generalized many of the ideas from random walks on groups to monoids.

Recall: A **monoid** is almost a group, but some elements may not have inverses.

Since elements may not have inverses, the walk may not be transitive.

# Random multiplicative walks on $\mathbb{Z}/n\mathbb{Z}$

Take $M = \mathbb{Z}/n\mathbb{Z}$, (operation: multiplication)

# Random multiplicative walks on $\mathbb{Z}/n\mathbb{Z}$

Take $M = \mathbb{Z}/n\mathbb{Z}$, (operation: multiplication) $S = \mathbb{Z}/n\mathbb{Z}$,

# Random multiplicative walks on $\mathbb{Z}/n\mathbb{Z}$

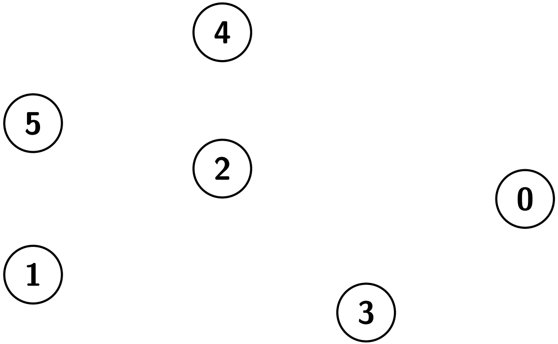
Take $M = \mathbb{Z}/n\mathbb{Z}$, (operation: multiplication) $S = \mathbb{Z}/n\mathbb{Z}$, $X_0 = 1$.

# Random multiplicative walks on $\mathbb{Z}/n\mathbb{Z}$

Take $M = \mathbb{Z}/n\mathbb{Z}$, (operation: multiplication) $S = \mathbb{Z}/n\mathbb{Z}$, $X_0 = 1$.
**Example:** Let $n = 6$.

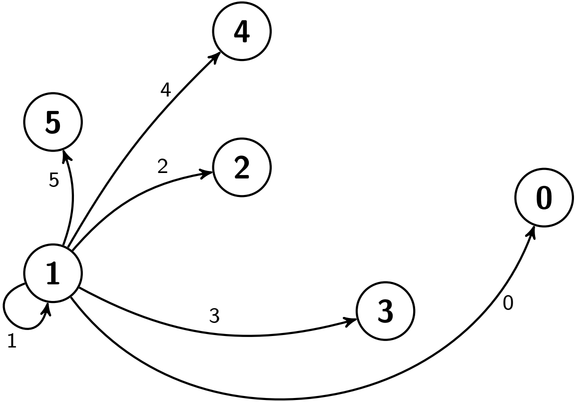
# Random multiplicative walks on $\mathbb{Z}/n\mathbb{Z}$

Take $M = \mathbb{Z}/n\mathbb{Z}$, (operation: multiplication) $S = \mathbb{Z}/n\mathbb{Z}$, $X_0 = 1$.
**Example:** Let $n = 6$.



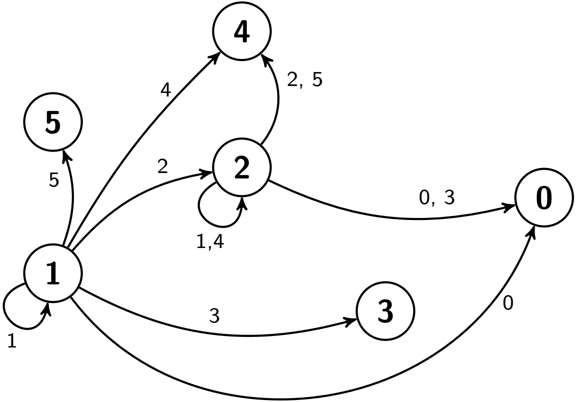
# Random multiplicative walks on $\mathbb{Z}/n\mathbb{Z}$

Take $M = \mathbb{Z}/n\mathbb{Z}$, (operation: multiplication) $S = \mathbb{Z}/n\mathbb{Z}$, $X_0 = 1$.
**Example:** Let $n = 6$.

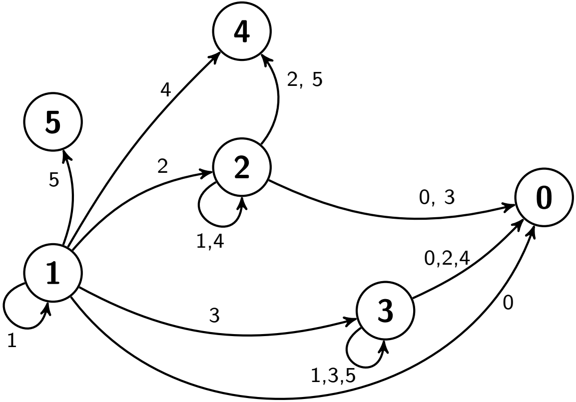


# Random multiplicative walks on $\mathbb{Z}/n\mathbb{Z}$

Take $M = \mathbb{Z}/n\mathbb{Z}$, (operation: multiplication) $S = \mathbb{Z}/n\mathbb{Z}$, $X_0 = 1$.
**Example:** Let $n = 6$.

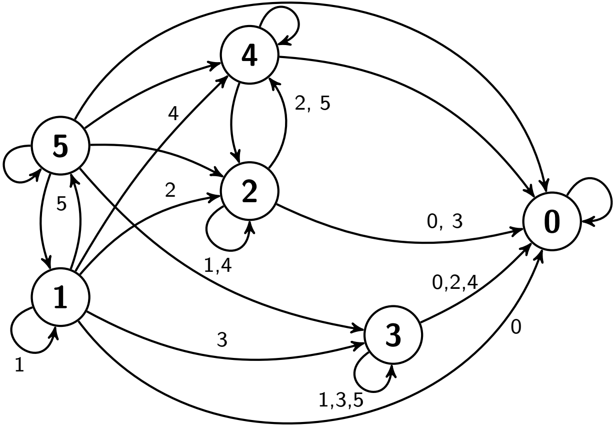


Take $M = \mathbb{Z}/n\mathbb{Z}$, (operation: multiplication) $S = \mathbb{Z}/n\mathbb{Z}$, $X_0 = 1$.
**Example:** Let $n = 6$.



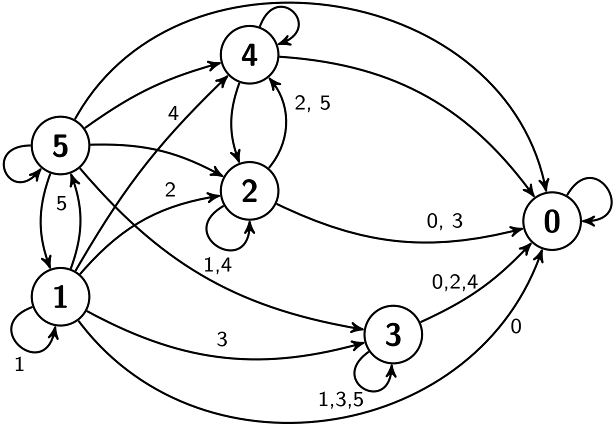
# Random multiplicative walks on $\mathbb{Z}/n\mathbb{Z}$

Take $M = \mathbb{Z}/n\mathbb{Z}$, (operation: multiplication) $S = \mathbb{Z}/n\mathbb{Z}$, $X_0 = 1$.
**Example:** Let $n = 6$.



# Random multiplicative walks on $\mathbb{Z}/n\mathbb{Z}$

Take $M = \mathbb{Z}/n\mathbb{Z}$, (operation: multiplication) $S = \mathbb{Z}/n\mathbb{Z}$, $X_0 = 1$.
**Example:** Let $n = 6$.




Single absorbing state: 0 (mod $n$).

# Random multiplicative walks on $\mathbb{Z}/n\mathbb{Z}$

For any integer $n$ this random walk will eventually reach the absorbing state $0 \pmod{n}$.

# Random multiplicative walks on $\mathbb{Z}/n\mathbb{Z}$

For any integer $n$ this random walk will eventually reach the absorbing state $0 \pmod{n}$.

Let $a(n) = \mathbb{E}[\text{Number of steps to reach } 0 \ (\text{mod } n)]$.

# Random multiplicative walks on $\mathbb{Z}/n\mathbb{Z}$

For any integer $n$ this random walk will eventually reach the absorbing state $0 \pmod{n}$.

Let $a(n) = \mathbb{E}[\text{Number of steps to reach } 0 \pmod{n}]$.

Alternatively: Start with the empty product: 1. Randomly multiply by integers chosen uniformly at random from $[1, n]$.

# Random multiplicative walks on $\mathbb{Z}/n\mathbb{Z}$

For any integer $n$ this random walk will eventually reach the absorbing state $0 \pmod{n}$.

Let $a(n) = \mathbb{E}[\text{Number of steps to reach } 0 \pmod{n}]$.

Alternatively: Start with the empty product: 1. Randomly multiply by integers chosen uniformly at random from $[1, n]$. $a(n)$ is the expected number of multiplications before $n$ divides the product.

# Random multiplicative walks on $\mathbb{Z}/n\mathbb{Z}$

For any integer $n$ this random walk will eventually reach the absorbing state $0 \pmod{n}$.

Let $a(n) = \mathbb{E}[\text{Number of steps to reach } 0 \pmod{n}]$.

Alternatively: Start with the empty product: 1. Randomly multiply by integers chosen uniformly at random from $[1, n]$. $a(n)$ is the expected number of multiplications before $n$ divides the product.

$a(6) =$

# Random multiplicative walks on $\mathbb{Z}/n\mathbb{Z}$

For any integer $n$ this random walk will eventually reach the absorbing state $0 \pmod{n}$.

Let $a(n) = \mathbb{E}[\text{Number of steps to reach } 0 \pmod{n}]$.

Alternatively: Start with the empty product: 1. Randomly multiply by integers chosen uniformly at random from $[1, n]$. $a(n)$ is the expected number of multiplications before $n$ divides the product.

$a(6) = 3.5$.

# Warm up

**Case:** $n = p$ is prime.

# Warm up

**Case:** $n = p$ is prime.
Every element besides $0 \pmod p$ is a unit.

# Warm up

**Case:** $n = p$ is prime.
Every element besides $0 \pmod p$ is a unit.
Each selection from $\mathbb{Z}/n\mathbb{Z}$ is a Bernoulli trial with probability

$$\begin{array}{ll} \frac{p-1}{p} & \text{Remain in } (\mathbb{Z}/n\mathbb{Z})^\times \\ \frac{1}{p} & \text{Step to } 0 \pmod p \end{array}$$

# Warm up

**Case:** $n = p$ is prime.
Every element besides $0 \pmod p$ is a unit.
Each selection from $\mathbb{Z}/n\mathbb{Z}$ is a Bernoulli trial with probability

$$\begin{array}{ll} \frac{p-1}{p} & \text{Remain in } (\mathbb{Z}/n\mathbb{Z})^\times \\ \frac{1}{p} & \text{Step to } 0 \pmod p \end{array}$$

$$a(p) = p$$

# Prime powers

**Case:** $n = p^k$ is a prime power.

# Prime powers

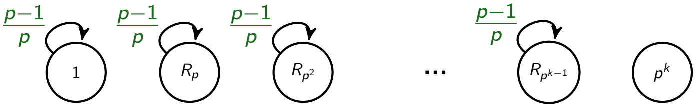
**Case:** $n = p^k$ is a prime power.
Let $R_d = \{r \in \mathbb{Z}/n\mathbb{Z} | (r, n) = d\}$.

# Prime powers

**Case:** $n = p^k$ is a prime power.
Let $R_d = \{r \in \mathbb{Z}/n\mathbb{Z} | (r, n) = d\}$.

# Prime powers

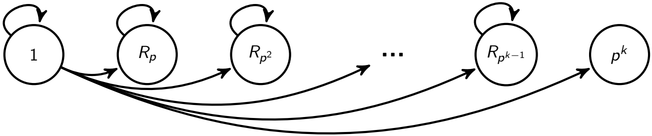
**Case:** $n = p^k$ is a prime power.
Let $R_d = \{r \in \mathbb{Z}/n\mathbb{Z} | (r, n) = d\}$.




The probability of selecting a unit is $\frac{p-1}{p}$.

# Prime powers

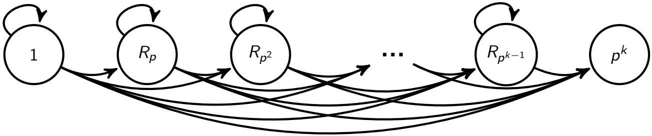
**Case:** $n = p^k$ is a prime power.
Let $R_d = \{r \in \mathbb{Z}/n\mathbb{Z} | (r, n) = d\}$.




The probability of selecting a unit is $\frac{p-1}{p}$.
The probability of transitioning from $R_1$ to $R_{p^i}$ is $\frac{p-1}{p^{i+1}}$ and to $R_{p^k}$ is $\frac{1}{p^k}$

# Prime powers

**Case:** $n = p^k$ is a prime power.
Let $R_d = \{r \in \mathbb{Z}/n\mathbb{Z} | (r, n) = d\}$.

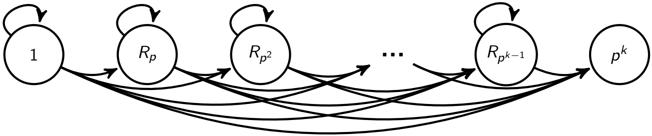



The probability of selecting a unit is $\frac{p-1}{p}$.
The probability of transitioning from $R_1$ to $R_{p^i}$ is $\frac{p-1}{p^{i+1}}$ and to $R_{p^k}$ is $\frac{1}{p^k}$

$$a(p^k) = \mathbb{E}[\text{Steps to first factor of } p] + \mathbb{E}[\text{Steps for remaining powers}]$$

# Prime powers

**Case:** $n = p^k$ is a prime power.
Let $R_d = \{r \in \mathbb{Z}/n\mathbb{Z} | (r, n) = d\}$.

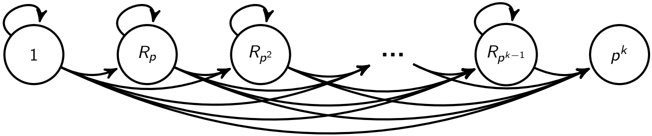



The probability of selecting a unit is $\frac{p-1}{p}$.
The probability of transitioning from $R_1$ to $R_{p^i}$ is $\frac{p-1}{p^{i+1}}$ and to $R_{p^k}$ is $\frac{1}{p^k}$

$$a(p^k) = \mathbb{E}[\text{Steps to first factor of } p] + \mathbb{E}[\text{Steps for remaining powers}]$$
$$= \quad p \quad + \quad \sum_{i=1}^{k-1} \left(\frac{p-1}{p^{i+1}}\right) a(p^i)$$

# Prime powers

**Case:** $n = p^k$ is a prime power.
Let $R_d = \{r \in \mathbb{Z}/n\mathbb{Z} | (r, n) = d\}$.




The probability of selecting a unit is $\frac{p-1}{p}$.
The probability of transitioning from $R_1$ to $R_{p^i}$ is $\frac{p-1}{p^{i+1}}$ and to $R_{p^k}$ is $\frac{1}{p^k}$

$$
\begin{aligned}
a(p^k) &= \mathbb{E}[\text{Steps to first factor of } p] + \mathbb{E}[\text{Steps for remaining powers}] \\
&= p + \sum_{i=1}^{k-1} \left(\frac{p-1}{p^{i+1}}\right) a(p^i) \\
&= k(p-1)+1
\end{aligned}
$$

# Arbitrary composite $n$

We can use a similar idea for arbitrary $n$:

# Arbitrary composite $n$

We can use a similar idea for arbitrary $n$:

$a(n) = \mathbb{E}[\text{Steps to first non-unit}] + \mathbb{E}[\text{Steps from there to } 0 \pmod{n}]$

# Arbitrary composite $n$

We can use a similar idea for arbitrary $n$:

$a(n) = \mathbb{E}[\text{Steps to first non-unit}] + \mathbb{E}[\text{Steps from there to } 0 \pmod{n}]$

$$\mathbb{E}[\text{Steps to first non-unit}] = \frac{n}{n - \varphi(n)}$$

# Arbitrary composite $n$

We can use a similar idea for arbitrary $n$:

$a(n) = \mathbb{E}[\text{Steps to first non-unit}] + \mathbb{E}[\text{Steps from there to } 0 \pmod{n}]$

$$\mathbb{E}[\text{Steps to first non-unit}] = \frac{n}{n - \varphi(n)}$$

$$\mathbb{P}(\text{First non-unit step to } R_d) = \frac{|R_d|}{n - \varphi(n)}$$

# Arbitrary composite $n$

We can use a similar idea for arbitrary $n$:

$a(n) = \mathbb{E}[\text{Steps to first non-unit}] + \mathbb{E}[\text{Steps from there to } 0 \pmod{n}]$

$$\mathbb{E}[\text{Steps to first non-unit}] = \frac{n}{n - \varphi(n)}$$

$$\mathbb{P}(\text{First non-unit step to } R_d) = \frac{|R_d|}{n - \varphi(n)} = \frac{\varphi\left(\frac{n}{d}\right)}{n - \varphi(n)}$$

# Arbitrary composite $n$

We can use a similar idea for arbitrary $n$:

$$a(n) = \mathbb{E}[\text{Steps to first non-unit}] + \mathbb{E}[\text{Steps from there to } 0 \pmod{n}]$$

$$\mathbb{E}[\text{Steps to first non-unit}] = \frac{n}{n - \varphi(n)}$$

$$\mathbb{P}(\text{First non-unit step to } R_d) = \frac{|R_d|}{n - \varphi(n)} = \frac{\varphi\left(\frac{n}{d}\right)}{n - \varphi(n)}$$

$$\mathbb{E}[\text{Steps from } R_d \text{ to } 0 \pmod{n}] = a\left(\frac{n}{d}\right)$$

# Arbitrary composite $n$

We can use a similar idea for arbitrary $n$:

$a(n) = \mathbb{E}[\text{Steps to first non-unit}] + \mathbb{E}[\text{Steps from there to } 0 \pmod{n}]$

$$\mathbb{E}[\text{Steps to first non-unit}] = \frac{n}{n-\varphi(n)}$$

$$\mathbb{P}(\text{First non-unit step to } R_d) = \frac{|R_d|}{n-\varphi(n)} = \frac{\varphi\left(\frac{n}{d}\right)}{n-\varphi(n)}$$

$$\mathbb{E}[\text{Steps from } R_d \text{ to } 0 \pmod{n}] = a\left(\frac{n}{d}\right)$$

$$a(n) = \frac{n}{n-\varphi(n)} + \sum_{\substack{d|n \\ d\neq 1}} \frac{\varphi\left(\frac{n}{d}\right) a\left(\frac{n}{d}\right)}{n-\varphi(n)}$$

# Arbitrary composite $n$

We can use a similar idea for arbitrary $n$:

$a(n) = \mathbb{E}[\text{Steps to first non-unit}] + \mathbb{E}[\text{Steps from there to } 0 \pmod{n}]$

$$\mathbb{E}[\text{Steps to first non-unit}] = \frac{n}{n - \varphi(n)}$$

$$\mathbb{P}(\text{First non-unit step to } R_d) = \frac{|R_d|}{n - \varphi(n)} = \frac{\varphi\left(\frac{n}{d}\right)}{n - \varphi(n)}$$

$$\mathbb{E}[\text{Steps from } R_d \text{ to } 0 \pmod{n}] = a\left(\frac{n}{d}\right)$$

$$a(n) = \frac{n}{n - \varphi(n)} + \sum_{\substack{d|n \\ d \neq 1}} \frac{\varphi\left(\frac{n}{d}\right) a\left(\frac{n}{d}\right)}{n - \varphi(n)} = \frac{1}{n - \varphi(n)} \left( n + \sum_{\substack{d|n \\ d \neq n}} \varphi(d)\, a(d) \right)$$

# Squarefree $n$

Suppose $n$ is squarefree.

# Squarefree $n$

Suppose $n$ is squarefree. For each $p|n$ let

$$X_p = \text{ number of steps before a residue chosen is divisible by } p.$$

# Squarefree $n$

Suppose $n$ is squarefree. For each $p|n$ let

$$X_p = \text{ number of steps before a residue chosen is divisible by } p.$$

- Independent.

# Squarefree $n$

Suppose $n$ is squarefree. For each $p|n$ let

$$X_p = \text{ number of steps before a residue chosen is divisible by } p.$$

- Independent.
- Geometrically distributed ($\mathbb{E}[X_p] = p$.)

# Squarefree $n$

Suppose $n$ is squarefree. For each $p|n$ let

$$X_p = \text{ number of steps before a residue chosen is divisible by } p.$$

- Independent.
- Geometrically distributed ($\mathbb{E}[X_p] = p$.)

$$a(n) = \mathbb{E}\left[\max_{p|n}\{X_p\}\right].$$

# Squarefree numbers

## Theorem

*For $n \geq 2$ squarefree,*

$$a(n) = \sum_{\substack{d|n \\ d\neq 1}} (-1)^{\omega(d)+1} \frac{d}{d - \varphi(d)}.$$

# Squarefree numbers

## Theorem

*For $n \geq 2$ squarefree,*
$$a(n) = \sum_{\substack{d|n \\ d\neq 1}} (-1)^{\omega(d)+1} \frac{d}{d - \varphi(d)}.$$

**Proof:** Let $X = \max_{p|n}\{X_p\}$.

# Squarefree numbers

## Theorem

*For $n \geq 2$ squarefree,* $$a(n) = \sum_{\substack{d|n \\ d \neq 1}} (-1)^{\omega(d)+1} \frac{d}{d - \varphi(d)}.$$

**Proof:** Let $X = \max_{p|n}\{X_p\}$.

$a(n) = \mathbb{E}[X]$

# Squarefree numbers

## Theorem

*For $n \geq 2$ squarefree,* $$a(n) = \sum_{\substack{d|n \\ d \neq 1}} (-1)^{\omega(d)+1} \frac{d}{d - \varphi(d)}.$$

**Proof:** Let $X = \max_{p|n}\{X_p\}$.

$$a(n) = \mathbb{E}[X] = \sum_{i=0}^{\infty} \mathbb{P}[X > i]$$

# Squarefree numbers

## Theorem

*For $n \geq 2$ squarefree,* $$a(n) = \sum_{\substack{d|n \\ d \neq 1}} (-1)^{\omega(d)+1} \frac{d}{d - \varphi(d)}.$$

**Proof:** Let $X = \max_{p|n}\{X_p\}$.

$$a(n) = \mathbb{E}[X] = \sum_{i=0}^{\infty} \mathbb{P}[X > i] = \sum_{i=0}^{\infty} (1 - \mathbb{P}[X \leq i])$$

# Squarefree numbers

## Theorem

*For $n \geq 2$ squarefree,*
$$a(n) = \sum_{\substack{d|n \\ d\neq 1}} (-1)^{\omega(d)+1} \frac{d}{d-\varphi(d)}.$$

**Proof:** Let $X = \max_{p|n}\{X_p\}$.

$$a(n) = \mathbb{E}[X] = \sum_{i=0}^{\infty} \mathbb{P}[X > i] = \sum_{i=0}^{\infty} (1 - \mathbb{P}[X \leq i])$$
$$= \sum_{i=0}^{\infty} \left(1 - \prod_{p|n} \mathbb{P}[X_p \leq i]\right)$$

# Squarefree numbers

## Theorem

*For $n \geq 2$ squarefree,* $$a(n) = \sum_{\substack{d|n \\ d \neq 1}} (-1)^{\omega(d)+1} \frac{d}{d - \varphi(d)}.$$

**Proof:** Let $X = \max_{p|n}\{X_p\}$.

$$a(n) = \mathbb{E}[X] = \sum_{i=0}^{\infty} \mathbb{P}[X > i] = \sum_{i=0}^{\infty} (1 - \mathbb{P}[X \leq i])$$
$$= \sum_{i=0}^{\infty} \left(1 - \prod_{p|n} \mathbb{P}[X_p \leq i]\right) = \sum_{i=0}^{\infty} \left(1 - \prod_{p|n} \left(1 - \left(\frac{p-1}{p}\right)^i\right)\right)$$

# Squarefree numbers

## Theorem

*For $n \geq 2$ squarefree,* $$a(n) = \sum_{\substack{d|n \\ d \neq 1}} (-1)^{\omega(d)+1} \frac{d}{d - \varphi(d)}.$$

**Proof:** Let $X = \max_{p|n}\{X_p\}$.

$$a(n) = \mathbb{E}[X] = \sum_{i=0}^{\infty} \mathbb{P}[X > i] = \sum_{i=0}^{\infty} (1 - \mathbb{P}[X \leq i])$$
$$= \sum_{i=0}^{\infty} \left(1 - \prod_{p|n} \mathbb{P}[X_p \leq i]\right) = \sum_{i=0}^{\infty} \left(1 - \prod_{p|n} \left(1 - \left(\frac{p-1}{p}\right)^i\right)\right)$$
$$= \sum_{i=0}^{\infty} \sum_{\substack{d|n \\ d \neq 1}} (-1)^{\omega(d)+1} \frac{\varphi(d)^i}{d^i}$$

# Squarefree numbers

## Theorem

*For $n \geq 2$ squarefree,* $$a(n) = \sum_{\substack{d|n \\ d\neq 1}} (-1)^{\omega(d)+1} \frac{d}{d-\varphi(d)}.$$

**Proof:** Let $X = \max_{p|n}\{X_p\}$.

$$a(n) = \mathbb{E}[X] = \sum_{i=0}^{\infty} \mathbb{P}[X > i] = \sum_{i=0}^{\infty} (1 - \mathbb{P}[X \leq i])$$
$$= \sum_{i=0}^{\infty} \left(1 - \prod_{p|n} \mathbb{P}[X_p \leq i]\right) = \sum_{i=0}^{\infty} \left(1 - \prod_{p|n}\left(1 - \left(\frac{p-1}{p}\right)^i\right)\right)$$
$$= \sum_{i=0}^{\infty} \sum_{\substack{d|n \\ d\neq 1}} (-1)^{\omega(d)+1} \frac{\varphi(d)^i}{d^i} = \sum_{\substack{d|n \\ d\neq 1}} \frac{(-1)^{\omega(d)+1}}{1 - \frac{\varphi(d)}{d}}$$

# Squarefree numbers

## Theorem

*For $n \geq 2$ squarefree,*
$$a(n) = \sum_{\substack{d|n \\ d\neq 1}} (-1)^{\omega(d)+1} \frac{d}{d-\varphi(d)}.$$

**Proof:** Let $X = \max_{p|n}\{X_p\}$.

$$a(n) = \mathbb{E}[X] = \sum_{i=0}^{\infty} \mathbb{P}[X > i] = \sum_{i=0}^{\infty} (1 - \mathbb{P}[X \leq i])$$
$$= \sum_{i=0}^{\infty} \left(1 - \prod_{p|n} \mathbb{P}[X_p \leq i]\right) = \sum_{i=0}^{\infty} \left(1 - \prod_{p|n} \left(1 - \left(\frac{p-1}{p}\right)^i\right)\right)$$
$$= \sum_{i=0}^{\infty} \sum_{\substack{d|n \\ d\neq 1}} (-1)^{\omega(d)+1} \frac{\varphi(d)^i}{d^i} = \sum_{\substack{d|n \\ d\neq 1}} \frac{(-1)^{\omega(d)+1}}{1 - \frac{\varphi(d)}{d}} = \sum_{\substack{d|n \\ d\neq 1}} (-1)^{\omega(d)+1} \frac{d}{d-\varphi(d)}.$$

# Bounds

Factor $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where $p_1 > p_2 > \ldots > p_k$.

# Bounds

Factor $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where $p_1 > p_2 > \ldots > p_k$.

Write

$$P_i(n) = p_i$$

# Bounds

Factor $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where $p_1 > p_2 > \ldots > p_k$.

Write

$$P_i(n) = p_i$$

$$B(n) = \sum_{i=1}^{k} \alpha_i p_i.$$

# Bounds

Factor $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where $p_1 > p_2 > \ldots > p_k$.

Write

$$P_i(n) = p_i$$

$$B(n) = \sum_{i=1}^{k} \alpha_i p_i.$$

Trivial lower bound:

$$P_1(n) \leq a(n).$$

# Bounds

Factor $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where $p_1 > p_2 > \ldots > p_k$.

Write

$$P_i(n) = p_i$$

$$B(n) = \sum_{i=1}^{k} \alpha_i p_i.$$

Trivial lower bound:

$$P_1(n) \leq a(n).$$

Almost-as-trivial upper bound:

$$a(n) \leq B(n).$$

# Bounds

$$P_1(n) \leq a(n) \leq B(n)$$

# Bounds

$$P_1(n) \leq a(n) \leq B(n)$$

**Theorem:** (Alladi, Erdős, 1977)

$$\sum_{n<x} P_1(n) \sim \frac{\pi^2 x^2}{12 \log x}$$

# Bounds

$$P_1(n) \leq a(n) \leq B(n)$$

**Theorem:** (Alladi, Erdős, 1977)

$$\sum_{n<x} P_1(n) \sim \frac{\pi^2 x^2}{12 \log x} \sim \sum_{n<x} B(n).$$

# Bounds

$$P_1(n) \le a(n) \le B(n)$$

**Theorem:** (Alladi, Erdős, 1977)

$$\sum_{n<x} P_1(n) \sim \frac{\pi^2 x^2}{12 \log x} \sim \sum_{n<x} B(n).$$

**Corollary:** $\displaystyle\sum_{n<x} a(n) \sim \frac{\pi^2 x^2}{12 \log x}.$

# Bounds

$$P_1(n) \le a(n) \le B(n)$$

**Theorem:** (Alladi, Erdős, 1977)

$$\sum_{n<x} P_1(n) \sim \frac{\pi^2 x^2}{12 \log x} \sim \sum_{n<x} B(n).$$

**Corollary:** $\displaystyle\sum_{n<x} a(n) \sim \frac{\pi^2 x^2}{12 \log x}.$

The asymptotic behavior of $P_i(n)$, $B(n)$ and their friends have been studied by Alladi, De Koninck, Erdős, Ivić, Naslund, Pomerance and others.

# Estimates

Is $P_1(n)$ or $B(n)$ a better estimate for $a(n)$?

# Estimates

Is $P_1(n)$ or $B(n)$ a better estimate for $a(n)$?

**Theorem**

*On a set of asymptotic density 1,*

# Estimates

Is $P_1(n)$ or $B(n)$ a better estimate for $a(n)$?

## Theorem

*On a set of asymptotic density 1,*

$$a(n) = P_1(n) + o(1) \qquad \text{If } P_1(n) > P_2(n)^2$$

# Estimates

Is $P_1(n)$ or $B(n)$ a better estimate for $a(n)$?

**Theorem**

*On a set of asymptotic density 1,*

$$a(n) = P_1(n) + o(1) \qquad \text{If } P_1(n) > P_2(n)^2$$
$$a(n) - P_1(n) \to \infty \text{ as } n \to \infty \qquad \text{If } P_1(n) < P_2(n)^2.$$

# Estimates

Is $P_1(n)$ or $B(n)$ a better estimate for $a(n)$?

**Theorem**

*On a set of asymptotic density 1,*

$$\begin{aligned} a(n) &= P_1(n) + o(1) && \text{If } P_1(n) > P_2(n)^2 \\ a(n) - P_1(n) &\to \infty \text{ as } n \to \infty && \text{If } P_1(n) < P_2(n)^2. \end{aligned}$$

**Theorem (Wheeler, 1990)**

*The integers with $P_1(n) > P_2(n)^2$ have density 0.62432... the Golomb-Dickman constant.*

# Average number of steps after the largest prime

# Average number of steps after the largest prime

**Theorem (Erdős, Alladi, 1977)**

$$\sum_{n \le x} (B(n) - P_1(n))$$

# Average number of steps after the largest prime

### Theorem (Erdős, Alladi, 1977)

$$\sum_{n \leq x} (B(n) - P_1(n)) \sim \sum_{n \leq x} P_2(n)$$

# Average number of steps after the largest prime

**Theorem (Erdős, Alladi, 1977)**

$$\sum_{n\le x} (B(n) - P_1(n)) \sim \sum_{n\le x} P_2(n) \sim K_2 \frac{x^{3/2}}{\log^2 x}$$

# Average number of steps after the largest prime

**Theorem (Erdős, Alladi, 1977)**

$$\sum_{n\le x}(B(n)-P_1(n)) \sim \sum_{n\le x} P_2(n) \sim K_2\frac{x^{3/2}}{\log^2 x}$$

**Balasubramanian:** $K_2=\frac{8}{3}\zeta(3/2)$.

# Average number of steps after the largest prime

$$\sum_{n\leq x} B(n) - P_1(n) \sim \sum_{n\leq x} P_2(n) \sim \frac{8}{3}\zeta(3/2)\frac{x^{3/2}}{\log^2 x}$$

# Average number of steps after the largest prime

$$\sum_{n\leq x} B(n) - P_1(n) \sim \sum_{n\leq x} P_2(n) \sim \frac{8}{3}\zeta(3/2)\frac{x^{3/2}}{\log^2 x}$$

What about $a(n) - P_1(n)$?

# Average number of steps after the largest prime

$$\sum_{n\leq x} B(n) - P_1(n) \sim \sum_{n\leq x} P_2(n) \sim \frac{8}{3}\zeta(3/2)\frac{x^{3/2}}{\log^2 x}$$

What about $a(n) - P_1(n)$? Note: This is the expected number of steps required after picking up the largest prime divisor of $n$.

# Average number of steps after the largest prime

$$\sum_{n\le x} B(n) - P_1(n) \sim \sum_{n\le x} P_2(n) \sim \frac{8}{3}\zeta(3/2)\frac{x^{3/2}}{\log^2 x}$$

What about $a(n) - P_1(n)$? Note: This is the expected number of steps required after picking up the largest prime divisor of $n$.

**Theorem**

$$\sum_{n\le x} a(n) - P_1(n) \sim \frac{8-2\pi}{3}\zeta(3/2)\frac{x^{3/2}}{\log^2 x}$$

# Average number of steps after the largest prime

$$\sum_{n\le x} B(n) - P_1(n) \sim \sum_{n\le x} P_2(n) \sim \frac{8}{3}\zeta(3/2)\frac{x^{3/2}}{\log^2 x}$$

What about $a(n) - P_1(n)$? Note: This is the expected number of steps required after picking up the largest prime divisor of $n$.

## Theorem

$$\sum_{n\le x} a(n) - P_1(n) \sim \frac{8-2\pi}{3}\zeta(3/2)\frac{x^{3/2}}{\log^2 x} \sim \left(1-\frac{\pi}{4}\right)\sum_{n\le x} P_2(n)$$

# Average number of steps after the largest prime

$$\sum_{n\le x} B(n) - P_1(n) \sim \sum_{n\le x} P_2(n) \sim \frac{8}{3}\zeta(3/2)\frac{x^{3/2}}{\log^2 x}$$

What about $a(n) - P_1(n)$? Note: This is the expected number of steps required after picking up the largest prime divisor of $n$.

## Theorem

$$\sum_{n\le x} a(n) - P_1(n) \sim \frac{8-2\pi}{3}\zeta(3/2)\frac{x^{3/2}}{\log^2 x} \sim \left(1 - \tfrac{\pi}{4}\right)\sum_{n\le x} P_2(n)$$

**"On average:"** $a(n) \approx P_1(n) + \left(1 - \frac{\pi}{4}\right) P_2(n)$.

# Further questions

# Further questions

**Question**

*Is $a(n)$ ever an integer when $n$ is not a prime or prime power?*

# Further questions

**Question**

*Is $a(n)$ ever an integer when $n$ is not a prime or prime power?*

**Question**

*How many distinct residues modulo $n$ is this walk expected to visit?*

# Further questions

## Question

*Is $a(n)$ ever an integer when $n$ is not a prime or prime power?*

## Question

*How many distinct residues modulo $n$ is this walk expected to visit?*

## Question

*Can similar results be obtained about the variance of the time to reach $0 \pmod{n}$?*

Thank you!