Reed-Solomon code.

**Problem:** Communicate $n$ packets $m_1, \ldots, m_n$ on noisy channel that corrupts $\leq k$ packets.
Reed-Solomon code.

**Problem:** Communicate $n$ packets $m_1, \ldots, m_n$ on noisy channel that corrupts $\leq k$ packets.

**Reed-Solomon Code:**

1. Make a polynomial, $P(x)$ of degree $n-1$, that encodes message: coefficients, $p_0, \ldots, p_{n-1}$.
2. Send $P(1), \ldots, P(n+2k)$.

After noisy channel: Receive values $R(1), \ldots, R(n+2k)$.

**Properties:**

1. $P(i) = R(i)$ for at least $n+k$ points $i$.
2. $P(x)$ is unique degree $n-1$ polynomial that contains $\geq n+k$ received points.

Matrix view of encoding: modulo $p$. 

$$
\begin{bmatrix}
P(1) \\
P(2) \\
P(3) \\
\vdots \\
P(n+2k)
\end{bmatrix}
= 
\begin{bmatrix}
1 & 1 & 1 & \ldots & 1 \\
2 \cdot 1 & 2 \cdot 1 & 2 \cdot 2 & \ldots & 2 \cdot (n-1) \\
3 \cdot 1 & 3 \cdot 2 & 3 \cdot 3 & \ldots & 3 \cdot (n-1) \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
(n+2k) \cdot 1 & (n+2k) \cdot 2 & (n+2k) \cdot 3 & \ldots & (n+2k) \cdot (n-1)
\end{bmatrix}
\begin{bmatrix}
p_0 \\
p_1 \\
p_2 \\
\vdots \\
p_{n-1}
\end{bmatrix}
\pmod{p}
$$
**Reed-Solomon code.**

**Problem:** Communicate $n$ packets $m_1, \ldots, m_n$ on noisy channel that corrupts $\leq k$ packets.

**Reed-Solomon Code:**

1. Make a polynomial, $P(x)$ of degree $n - 1$, that encodes message: coefficients, $p_0, \ldots, p_{n-1}$.
Reed-Solomon code.

**Problem:** Communicate $n$ packets $m_1, \ldots, m_n$ on noisy channel that corrupts $\leq k$ packets.

**Reed-Solomon Code:**

1. Make a polynomial, $P(x)$ of degree $n-1$, that encodes message: coefficients, $p_0, \ldots, p_{n-1}$.
2. Send $P(1), \ldots, P(n+2k)$. 
Reed-Solomon code.

**Problem:** Communicate $n$ packets $m_1, \ldots, m_n$ on noisy channel that corrupts $\leq k$ packets.

**Reed-Solomon Code:**

1. Make a polynomial, $P(x)$ of degree $n - 1$, that encodes message: coefficients, $p_0, \ldots, p_{n-1}$.

2. Send $P(1), \ldots, P(n+2k)$.

**After noisy channel:** Receive values $R(1), \ldots, R(n+2k)$. 
Reed-Solomon code.

**Problem:** Communicate $n$ packets $m_1, \ldots, m_n$ on noisy channel that corrupts $\leq k$ packets.

**Reed-Solomon Code:**

1. Make a polynomial, $P(x)$ of degree $n - 1$, that encodes message: coefficients, $p_0, \ldots, p_{n-1}$.
2. Send $P(1), \ldots, P(n+2k)$.

**After noisy channel:** Receive values $R(1), \ldots, R(n+2k)$.

**Properties:**

1. $P(i) = R(i)$ for at least $n + k$ points $i$,\
Reed-Solomon code.

**Problem:** Communicate \( n \) packets \( m_1, \ldots, m_n \) on noisy channel that corrupts \( \leq k \) packets.

**Reed-Solomon Code:**

1. Make a polynomial, \( P(x) \) of degree \( n - 1 \), that encodes message: coefficients, \( p_0, \ldots, p_{n-1} \).

2. Send \( P(1), \ldots, P(n + 2k) \).

**After noisy channel:** Receive values \( R(1), \ldots, R(n + 2k) \).

**Properties:**

(1) \( P(i) = R(i) \) for at least \( n + k \) points \( i \),

(2) \( P(x) \) is unique degree \( n - 1 \) polynomial
Reed-Solomon code.

**Problem:** Communicate \( n \) packets \( m_1, \ldots, m_n \) on noisy channel that corrupts \( \leq k \) packets.

**Reed-Solomon Code:**

1. Make a polynomial, \( P(x) \) of degree \( n - 1 \), that encodes message: coefficients, \( p_0, \ldots, p_{n-1} \).
2. Send \( P(1), \ldots, P(n+2k) \).

**After noisy channel:** Recieve values \( R(1), \ldots, R(n+2k) \).

**Properties:**

(1) \( P(i) = R(i) \) for at least \( n + k \) points \( i \),

(2) \( P(x) \) is unique degree \( n - 1 \) polynomial that contains \( \geq n + k \) received points.
Reed-Solomon code.

**Problem:** Communicate \(n\) packets \(m_1, \ldots, m_n\) on noisy channel that corrupts \(\leq k\) packets.

**Reed-Solomon Code:**

1. Make a polynomial, \(P(x)\) of degree \(n - 1\), that encodes message: coefficients, \(p_0, \ldots, p_{n-1}\).

2. Send \(P(1), \ldots, P(n+2k)\).

**After noisy channel:** Recieve values \(R(1), \ldots, R(n+2k)\).

**Properties:**

1. \(P(i) = R(i)\) for at least \(n + k\) points \(i\),
2. \(P(x)\) is unique degree \(n - 1\) polynomial that contains \(\geq n + k\) received points.

Matrix view of encoding: modulo \(p\).
Reed-Solomon code.

**Problem:** Communicate \( n \) packets \( m_1, \ldots, m_n \) on noisy channel that corrupts \( \leq k \) packets.

**Reed-Solomon Code:**

1. Make a polynomial, \( P(x) \) of degree \( n - 1 \), that encodes message: coefficients, \( p_0, \ldots, p_{n-1} \).
2. Send \( P(1), \ldots, P(n+2k) \).

**After noisy channel:** Recieve values \( R(1), \ldots, R(n+2k) \).

**Properties:**

(1) \( P(i) = R(i) \) for at least \( n + k \) points \( i \),

(2) \( P(x) \) is unique degree \( n - 1 \) polynomial that contains \( \geq n + k \) received points.

**Matrix view of encoding:** modulo \( p \).

\[
\begin{bmatrix}
P(1) \\
P(2) \\
P(3) \\
\vdots \\
P(n+2k)
\end{bmatrix} = \begin{bmatrix}
1 & 1 & 1^2 & \cdots & 1^{2^{n-1}} \\
1 & 2 & 2^2 & \cdots & 2^{n-1} \\
1 & 3 & 3^2 & \cdots & 3^{n-1} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & (n+2k) & (n+2k)^2 & \cdots & (n+2k)^{n-1}
\end{bmatrix} \begin{bmatrix}
p_0 \\
p_1 \\
\vdots \\
p_{n-1}
\end{bmatrix} \pmod{p}
\]
Berlekamp-Welsh Algorithm

\[ P(x) : \text{degree } n - 1 \text{ polynomial.} \]
Berlekamp-Welsh Algorithm

\[ P(x) : \text{degree } n - 1 \text{ polynomial.} \]
Send \( P(1), \ldots, P(n + 2k) \)
Berlekamp-Welsh Algorithm

\[ P(x) \text{: degree } n - 1 \text{ polynomial.} \]
Send \[ P(1), \ldots, P(n + 2k) \]
Receive \[ R(1), \ldots, R(n + 2k) \]

Idea:
\[ E(x) \text{ is error locator polynomial.} \]
Root at each error point.
Degree \( k \).
\[ Q(x) = P(x)E(x) \text{ or degree } n + k - 1 \text{ polynomial.} \]
Set up system corresponding to
\[ Q(i) = R(i)E(i) \]
where \( Q(x) \) is degree \( n + k - 1 \) polynomial.
Coefficients:
\[ a_0, \ldots, a_{n + k - 1} \]
\[ E(x) \text{ is degree } k \text{ polynomial.} \]
Coefficients:
\[ b_0, \ldots, b_{k - 1}, 1 \]
Matrix equations: modulo \( p! \)
\[
\begin{bmatrix}
1 & 1 \\
1 & 2 \\
\vdots & \vdots \\
1 & (n + 2k)
\end{bmatrix}
\begin{bmatrix}
a_0 \\
a_1 \\
\vdots \\
a_{n + k - 1}
\end{bmatrix} =
\begin{bmatrix}
R(1) \\
R(2) \\
\vdots \\
R(n + 2k)
\end{bmatrix}
\]
Solve.
Then output \( P(x) = Q(x) / E(x) \).
Berlekamp-Welsh Algorithm

$P(x)$: degree $n - 1$ polynomial.
Send $P(1), \ldots, P(n + 2k)$
Receive $R(1), \ldots, R(n + 2k)$
At most $k$ i’s where $P(i) \neq R(i)$. 
Berlekamp-Welsh Algorithm

$P(x)$: degree $n - 1$ polynomial.
Send $P(1), \ldots, P(n + 2k)$
Receive $R(1), \ldots, R(n + 2k)$
At most $k$ i’s where $P(i) \neq R(i)$. 
Berlekamp-Welsh Algorithm

\( P(x) \): degree \( n - 1 \) polynomial.
Send \( P(1), \ldots, P(n + 2k) \)
Receive \( R(1), \ldots, R(n + 2k) \)
At most \( k \) i’s where \( P(i) \neq R(i) \).

Idea:

\[ E(x) \text{ is error locator polynomial.} \]
\[ \text{Root at each error point.} \]
\[ Q(x) = P(x) E(x) \text{ or degree } n + k - 1 \text{ polynomial.} \]
\[ \text{Set up system corresponding to } Q(x) = R(x) E(x) \text{ where } Q(x) \text{ is degree } n + k - 1 \text{ polynomial.} \]
\[ \text{Coefficients: } a_0, \ldots, a_{n+k-1} \]
\[ \text{Coefficients: } b_0, \ldots, b_{k-1}, 1 \]
Matrix equations: modulo \( p! \)
\[
\begin{array}{cccc}
1 & 1 & \cdots & 1 \\
1 & 2 & \cdots & 2 \\
\vdots & \vdots & \ddots & \vdots \\
1 & n+2k & \cdots & n+2k \\
\end{array}
\begin{array}{c}
a_0 \\
a_1 \\
\vdots \\
a_{n+k-1} \\
\end{array}
= 
\begin{array}{c}
R(1) \\
R(2) \\
\vdots \\
R(n+2k) \\
\end{array}
\begin{array}{c}
1 \\
1 \\
\vdots \\
1 \\
\end{array}
\begin{array}{c}
b_0 \\
b_1 \\
\vdots \\
b_{k-1} \\
1 \\
\end{array}
\]
Solve.
Then output \( P(x) = Q(x) / E(x) \).
Berlekamp-Welsh Algorithm

$P(x)$: degree $n-1$ polynomial.
Send $P(1), \ldots, P(n+2k)$
Receive $R(1), \ldots, R(n+2k)$
At most $k$ $i$'s where $P(i) \neq R(i)$.

Idea:
$E(x)$ is error locator polynomial.
Berlekamp-Welsh Algorithm

\[ P(x) : \text{degree } n - 1 \text{ polynomial}. \]
Send \( P(1), \ldots, P(n + 2k) \)
Receive \( R(1), \ldots, R(n + 2k) \)
At most \( k \) i’s where \( P(i) \neq R(i) \).

Idea:
\( E(x) \) is error locator polynomial.
\( E(x) \) is degree \( k \) polynomial.
Root at each error point.

Set up system corresponding to
\[ Q(x) = P(x)E(x) \text{ or degree } n + k - 1 \text{ polynomial}. \]

Matrix equations: modulo \( p! \)
\[
\begin{bmatrix}
1 & 1 & \cdots & 1 \\
1 & 2 & \cdots & 2(n + 2k) \\
\vdots & \vdots & \ddots & \vdots \\
1 & (n + 2k) & \cdots & (n + 2k)
\end{bmatrix}
\begin{bmatrix}
a_0 \\
a_1 \\
\vdots \\
a_{n + k - 1}
\end{bmatrix}
= 
\begin{bmatrix}
R(1) \\
R(2) \\
\vdots \\
R(n + 2k)
\end{bmatrix}
\]

Solve.
Then output
\[ P(x) = \frac{Q(x)}{E(x)}. \]
Berlekamp-Welsh Algorithm

\( P(x) \): degree \( n - 1 \) polynomial.
Send \( P(1), \ldots, P(n + 2k) \)
Receive \( R(1), \ldots, R(n + 2k) \)
At most \( k \) \( i \)'s where \( P(i) \neq R(i) \).

Idea:
\( E(x) \) is error locator polynomial.
Root at each error point. Degree \( k \).
\( Q(x) = P(x)E(x) \) or degree \( n + k - 1 \) polynomial.
**Berlekamp-Welsh Algorithm**

\[ P(x) \]: degree \( n - 1 \) polynomial.

Send \( P(1), \ldots, P(n + 2k) \)

Receive \( R(1), \ldots, R(n + 2k) \)

At most \( k \) i’s where \( P(i) \neq R(i) \).

Idea:

\( E(x) \) is error locator polynomial.

Root at each error point. Degree \( k \).

\[ Q(x) = P(x)E(x) \] or degree \( n + k - 1 \) polynomial.

Set up system corresponding to \( Q(i) = R(i)E(i) \) where
Berlekamp-Welsh Algorithm

\( P(x) \): degree \( n - 1 \) polynomial.
Send \( P(1), \ldots, P(n + 2k) \)
Receive \( R(1), \ldots, R(n + 2k) \)
At most \( k \) \( i \)'s where \( P(i) \neq R(i) \).

Idea:
\( E(x) \) is error locator polynomial.
\( \text{Root at each error point. Degree } k. \)
\( Q(x) = P(x)E(x) \) or degree \( n + k - 1 \) polynomial.

Set up system corresponding to \( Q(i) = R(i)E(i) \) where
\( Q(x) \) is degree \( n + k - 1 \) polynomial.
Berlekamp-Welsh Algorithm

\(P(x)\): degree \(n - 1\) polynomial.
Send \(P(1), \ldots, P(n+2k)\)
Receive \(R(1), \ldots, R(n+2k)\)
At most \(k\) \(i\)'s where \(P(i) \neq R(i)\).

Idea:

\(E(x)\) is error locator polynomial.
- Root at each error point. Degree \(k\).

\(Q(x) = P(x)E(x)\) or degree \(n+k-1\) polynomial.

Set up system corresponding to \(Q(i) = R(i)E(i)\) where
- \(Q(x)\) is degree \(n+k-1\) polynomial. Coefficients: \(a_0, \ldots, a_{n+k-1}\)
Berlekamp-Welsh Algorithm

\[ P(x): \text{degree } n - 1 \text{ polynomial.} \]
Send \( P(1), \ldots, P(n+2k) \)
Receive \( R(1), \ldots, R(n+2k) \)
At most \( k \) i’s where \( P(i) \neq R(i) \).

Idea:
\( E(x) \) is error locator polynomial.
Root at each error point. Degree \( k \).
\[ Q(x) = P(x)E(x) \text{ or degree } n + k - 1 \text{ polynomial.} \]

Set up system corresponding to \( Q(i) = R(i)E(i) \) where
\( Q(x) \) is degree \( n + k - 1 \) polynomial. Coefficients: \( a_0, \ldots, a_{n+k-1} \)
\( E(x) \) is degree \( k \) polynomial.
Berlekamp-Welsh Algorithm

\[ P(x) \]: degree \( n - 1 \) polynomial.
Send \( P(1), \ldots, P(n + 2k) \)
Receive \( R(1), \ldots, R(n + 2k) \)
At most \( k \) i’s where \( P(i) \neq R(i) \).

Idea:
\( E(x) \) is error locator polynomial.
Root at each error point. Degree \( k \).
\[ Q(x) = P(x)E(x) \] or degree \( n + k - 1 \) polynomial.

Set up system corresponding to \( Q(i) = R(i)E(i) \) where
\( Q(x) \) is degree \( n + k - 1 \) polynomial. Coefficients: \( a_0, \ldots, a_{n+k-1} \)
\( E(x) \) is degree \( k \) polynomial. Coefficients: \( b_0, \ldots, b_{k-1}, 1 \)
Berlekamp-Welsh Algorithm

\( P(x) \): degree \( n - 1 \) polynomial.
Send \( P(1), \ldots, P(n+2k) \)
Receive \( R(1), \ldots, R(n+2k) \)
At most \( k \) i’s where \( P(i) \neq R(i) \).

Idea:
\( E(x) \) is error locator polynomial.
Root at each error point. Degree \( k \).
\( Q(x) = P(x)E(x) \) or degree \( n + k - 1 \) polynomial.

Set up system corresponding to \( Q(i) = R(i)E(i) \) where
\( Q(x) \) is degree \( n + k - 1 \) polynomial. Coefficients: \( a_0, \ldots, a_{n+k-1} \)
\( E(x) \) is degree \( k \) polynomial. Coefficients: \( b_0, \ldots, b_{k-1}, 1 \)

Matrix equations: modulo \( p \)!
Berlekamp-Welsh Algorithm

\[ P(x) \text{: degree } n - 1 \text{ polynomial.} \]

Send \( P(1), \ldots, P(n+2k) \)
Receive \( R(1), \ldots, R(n+2k) \)
At most \( k \) i's where \( P(i) \neq R(i) \).

Idea:

\( E(x) \) is error locator polynomial.

Root at each error point. Degree \( k \).

\( Q(x) = P(x)E(x) \) or degree \( n + k - 1 \) polynomial.

Set up system corresponding to \( Q(i) = R(i)E(i) \) where

- \( Q(x) \) is degree \( n + k - 1 \) polynomial. Coefficients: \( a_0, \ldots, a_{n+k-1} \)
- \( E(x) \) is degree \( k \) polynomial. Coefficients: \( b_0, \ldots, b_{k-1}, 1 \)

Matrix equations: modulo \( p \! \)

\[
\begin{bmatrix}
1 & 1 & \cdots & 1 \\
1 & 2 & \cdots & 2^{n+k-1} \\
1 & 3 & \cdots & 3^{n+k-1} \\
\vdots & \vdots & \ddots & \vdots \\
1 & (n+2k) & \cdots & (n+2k)^{n+k-1}
\end{bmatrix}
\begin{bmatrix}
a_0 \\
a_1 \\
\vdots \\
a_{n+k-1}
\end{bmatrix}
= 
\begin{bmatrix}
R(1) & \cdots & 0 \\
0 & \cdots & 0 \\
\vdots & \ddots & \vdots \\
0 & \cdots & R(n+2k)
\end{bmatrix}
\begin{bmatrix}
1 & \cdots & 1 \\
1 & \cdots & 2^k \\
\vdots & \vdots & \vdots \\
1 & \cdots & (n+2k)^k
\end{bmatrix}
\begin{bmatrix}
b_0 \\
b_1 \\
\vdots \\
b_{k-1}
\end{bmatrix}
\]
Berlekamp-Welsh Algorithm

\( P(x) \): degree \( n - 1 \) polynomial.
Send \( P(1), \ldots, P(n + 2k) \)
Receive \( R(1), \ldots, R(n + 2k) \)
At most \( k \) i’s where \( P(i) \neq R(i) \).

Idea:
\( E(x) \) is error locator polynomial.
Root at each error point. Degree \( k \).
\( Q(x) = P(x)E(x) \) or degree \( n + k - 1 \) polynomial.

Set up system corresponding to \( Q(i) = R(i)E(i) \) where
\( Q(x) \) is degree \( n + k - 1 \) polynomial. Coefficients: \( a_0, \ldots, a_{n+k-1} \)
\( E(x) \) is degree \( k \) polyonimal. Coefficients: \( b_0, \ldots, b_{k-1}, 1 \)

Matrix equations: modulo \( p! \)

\[
\begin{bmatrix}
1 & 1 & \cdots & 1 \\
1 & 2 & \cdots & 2^{n+k-1} \\
1 & 3 & \cdots & 3^{n+k-1} \\
\vdots & \vdots & \ddots & \vdots \\
1 & (n+2k) & \cdots & (n+2k)^{n+k-1}
\end{bmatrix}
\begin{bmatrix}
a_0 \\
a_1 \\
a_n \\
\vdots \\
a_{n+k-1}
\end{bmatrix}
= \begin{bmatrix}
R(1) & \cdots & 0 \\
0 & \cdots & R(n+2k) \\
\vdots & \ddots & \vdots \\
1 & \cdots & 1
\end{bmatrix}
\begin{bmatrix}
b_0 \\
b_1 \\
b_k \\
\vdots \\
b_{k-1}
\end{bmatrix}
\]

Solve.
Berlekamp-Welsh Algorithm

$P(x)$: degree $n - 1$ polynomial.
Send $P(1), \ldots, P(n + 2k)$
Receive $R(1), \ldots, R(n + 2k)$
At most $k$ i’s where $P(i) \neq R(i)$.

Idea:
$E(x)$ is error locator polynomial.
Root at each error point. Degree $k$.
$Q(x) = P(x)E(x)$ or degree $n + k - 1$ polynomial.

Set up system corresponding to $Q(i) = R(i)E(i)$ where
$Q(x)$ is degree $n + k - 1$ polynomial. Coefficients: $a_0, \ldots, a_{n+k-1}$
$E(x)$ is degree $k$ polynomial. Coefficients: $b_0, \ldots, b_{k-1}, 1$

Matrix equations: modulo $p!$

$$\begin{pmatrix}
1 & 1 & 1 \\
1 & 2 & 2^{n+k-1} \\
1 & 3 & 3^{n+k-1} \\
. & . & . \\
1 & (n+2k) & (n+2k)^{n+k-1}
\end{pmatrix}
\begin{pmatrix}
a_0 \\
a_1 \\
. \\
. \\
a_{n+k-1}
\end{pmatrix}
= \begin{pmatrix}
R(1) & . & 0 \\
0 & . & 0 \\
. & . & . \\
. & . & . \\
0 & . & R(n+2k)
\end{pmatrix}
\begin{pmatrix}
1 & 1 & 1 \\
1 & 2^k & 3^k \\
. & . & . \\
. & . & . \\
1 & (n+2k)^k & 1
\end{pmatrix}
\begin{pmatrix}
b_0 \\
b_1 \\
. \\
. \\
b_{k-1}
\end{pmatrix}$$

Solve. Then output $P(x) = Q(x)/E(x)$. 
Finding $Q(x)$ and $E(x)$?
Finding $Q(x)$ and $E(x)$?

- $E(x)$ has degree $k$
Finding $Q(x)$ and $E(x)$?

- $E(x)$ has degree $k$ ...

$$E(x) = x^k + b_{k-1}x^{k-1} \cdots b_0.$$
Finding $Q(x)$ and $E(x)$?

- $E(x)$ has degree $k$ ...

\[
E(x) = x^k + b_{k-1}x^{k-1} \cdots b_0.
\]

$\implies k$ (unknown) coefficients.
Finding $Q(x)$ and $E(x)$?

- $E(x)$ has degree $k$ ...

\[ E(x) = x^k + b_{k-1}x^{k-1} \cdots b_0. \]

$\implies$ $k$ (unknown) coefficients. Leading coefficient is 1.
Finding $Q(x)$ and $E(x)$?

- $E(x)$ has degree $k$...

$$E(x) = x^k + b_{k-1}x^{k-1} \cdots b_0.$$  

$\implies k$ (unknown) coefficients. Leading coefficient is 1.

- $Q(x) = P(x)E(x)$ has degree $n + k - 1$
Finding $Q(x)$ and $E(x)$?

- $E(x)$ has degree $k$ ...

\[ E(x) = x^k + b_{k-1}x^{k-1} \cdots b_0. \]

\[ \implies k \text{ (unknown) coefficients. Leading coefficient is 1}. \]

- $Q(x) = P(x)E(x)$ has degree $n + k - 1$ ...

\[ Q(x) = a_{n+k-1}x^{n+k-1} + a_{n+k-2}x^{n+k-2} + \cdots a_0 \]
Finding $Q(x)$ and $E(x)$?

- $E(x)$ has degree $k$ ...

$$E(x) = x^k + b_{k-1}x^{k-1} \cdots b_0.$$  

$\implies k$ (unknown) coefficients. Leading coefficient is 1.

- $Q(x) = P(x)E(x)$ has degree $n + k - 1$ ...

$$Q(x) = a_{n+k-1}x^{n+k-1} + a_{n+k-2}x^{n+k-2} + \cdots a_0$$  

$\implies n + k$ (unknown) coefficients.
Finding $Q(x)$ and $E(x)$?

- $E(x)$ has degree $k$ ...

$$E(x) = x^k + b_{k-1}x^{k-1} \cdots b_0.$$  

$\implies k$ (unknown) coefficients. Leading coefficient is 1.

- $Q(x) = P(x)E(x)$ has degree $n+k-1$ ...

$$Q(x) = a_{n+k-1}x^{n+k-1} + a_{n+k-2}x^{n+k-2} + \cdots a_0$$  

$\implies n+k$ (unknown) coefficients.

Total unknown coefficient:
Finding $Q(x)$ and $E(x)$?

- $E(x)$ has degree $k$ ...

\[ E(x) = x^k + b_{k-1}x^{k-1} \cdots b_0. \]

$\implies k$ (unknown) coefficients. Leading coefficient is 1.

- $Q(x) = P(x)E(x)$ has degree $n + k - 1$ ...

\[ Q(x) = a_{n+k-1}x^{n+k-1} + a_{n+k-2}x^{n+k-2} + \cdots a_0 \]

$\implies n + k$ (unknown) coefficients.

Total unknown coefficient: \( n + 2k \).
Solving for $Q(x)$ and $E(x)$...

For all points $1, \ldots, i, n + 2k$,

$$Q(i) = R(i)E(i) \pmod{p}$$
Solving for \( Q(x) \) and \( E(x) \)...

For all points \( 1, \ldots, i, n+2k \),

\[
Q(i) = R(i)E(i) \pmod{p}
\]

Gives \( n+2k \) linear equations.
Solving for $Q(x)$ and $E(x)$...

For all points $1, \ldots, i, n + 2k$,

$$Q(i) = R(i)E(i) \pmod{p}$$

Gives $n + 2k$ linear equations.

$$a_{n+k-1} + \cdots a_0 \equiv R(1)(1 + b_{k-1} \cdots b_0) \pmod{p}$$
Solving for $Q(x)$ and $E(x)$...

For all points $1, \ldots, i, n + 2k$,

$$Q(i) = R(i)E(i) \pmod{p}$$

Gives $n + 2k$ linear equations.

$$a_{n+k-1} + \ldots a_0 \equiv R(1)(1 + b_{k-1} \cdots b_0) \pmod{p}$$

$$a_{n+k-1}(2)\ldots a_0 \equiv R(2)((2)^k + b_{k-1}(2)\ldots b_0) \pmod{p}$$

$$\vdots$$
Solving for $Q(x)$ and $E(x)$...

For all points $1, \ldots, i, n+2k$,

$$Q(i) = R(i)E(i) \pmod{p}$$

Gives $n+2k$ linear equations.

$$a_{n+k-1} + \cdots a_0 \equiv R(1)(1 + b_{k-1} \cdots b_0) \pmod{p}$$

$$a_{n+k-1}(2)^{n+k-1} + \cdots a_0 \equiv R(2)((2)^k + b_{k-1}(2)^{k-1} \cdots b_0) \pmod{p}$$

$$\vdots$$

$$a_{n+k-1}(m)^{n+k-1} + \cdots a_0 \equiv R(m)((m)^k + b_{k-1}(m)^{k-1} \cdots b_0) \pmod{p}$$
Solving for $Q(x)$ and $E(x)$...

For all points $1, \ldots, i, n+2k$,

$$Q(i) = R(i)E(i) \pmod{p}$$

Gives $n+2k$ linear equations.

$$a_{n+k-1} + \ldots a_0 \equiv R(1)(1 + b_{k-1} \cdots b_0) \pmod{p}$$

$$a_{n+k-1}(2)^{n+k-1} + \ldots a_0 \equiv R(2)((2)^k + b_{k-1}(2)^{k-1} \cdots b_0) \pmod{p}$$

$$\vdots$$

$$a_{n+k-1}(m)^{n+k-1} + \ldots a_0 \equiv R(m)((m)^k + b_{k-1}(m)^{k-1} \cdots b_0) \pmod{p}$$

..and $n+2k$ unknown coefficients of $Q(x)$ and $E(x)$!
Solving for $Q(x)$ and $E(x)$...

For all points $1, \ldots, i, n+2k$,

$$Q(i) = R(i)E(i) \pmod{p}$$

Gives $n+2k$ linear equations.

$$a_{n+k-1} + \cdots a_0 \equiv R(1)(1 + b_{k-1} \cdots b_0) \pmod{p}$$
$$a_{n+k-1}(2)^{n+k-1} + \cdots a_0 \equiv R(2)((2)^k + b_{k-1}(2)^{k-1} \cdots b_0) \pmod{p}$$
\[ \vdots \]
$$a_{n+k-1}(m)^{n+k-1} + \cdots a_0 \equiv R(m)((m)^k + b_{k-1}(m)^{k-1} \cdots b_0) \pmod{p}$$

..and $n+2k$ unknown coefficients of $Q(x)$ and $E(x)$!

Solve for coefficients of $Q(x)$ and $E(x)$. 

Solving for $Q(x)$ and $E(x)$...and $P(x)$

For all points $1, \ldots, i, n+2k$,

$$Q(i) = R(i)E(i) \pmod{p}$$

Gives $n+2k$ linear equations.

$$a_{n+k-1} + \ldots a_0 \equiv R(1)(1 + b_{k-1} \ldots b_0) \pmod{p}$$
$$a_{n+k-1}(2)^{n+k-1} + \ldots a_0 \equiv R(2)((2)^k + b_{k-1}(2)^{k-1} \ldots b_0) \pmod{p}$$
$$\vdots$$
$$a_{n+k-1}(m)^{n+k-1} + \ldots a_0 \equiv R(m)((m)^k + b_{k-1}(m)^{k-1} \ldots b_0) \pmod{p}$$

..and $n+2k$ unknown coefficients of $Q(x)$ and $E(x)$!

Solve for coefficients of $Q(x)$ and $E(x)$.

$$\text{Find } P(x) = Q(x)/E(x).$$
Solving for $Q(x)$ and $E(x)$...and $P(x)$

For all points $1, \ldots, i, n+2k$,

$$Q(i) = R(i)E(i) \pmod{p}$$

Gives $n+2k$ linear equations.

$$a_{n+k-1} + \cdots + a_0 \equiv R(1)(1 + b_{k-1} \cdots b_0) \pmod{p}$$

$$a_{n+k-1}(2)^{n+k-1} + \cdots + a_0 \equiv R(2)((2)^k + b_{k-1}(2)^{k-1} \cdots b_0) \pmod{p}$$

$$\vdots$$

$$a_{n+k-1}(m)^{n+k-1} + \cdots + a_0 \equiv R(m)((m)^k + b_{k-1}(m)^{k-1} \cdots b_0) \pmod{p}$$

..and $n+2k$ unknown coefficients of $Q(x)$ and $E(x)$!

Solve for coefficients of $Q(x)$ and $E(x)$.

Find $P(x) = Q(x)/E(x)$. 
Solving for $Q(x)$ and $E(x)$...and $P(x)$

For all points $1, \ldots, i, n+2k$,

$$Q(i) = R(i)E(i) \pmod{p}$$

Gives $n+2k$ linear equations.

$$a_{n+k-1} + \ldots + a_0 \equiv R(1)(1 + b_{k-1} \cdots b_0) \pmod{p}$$
$$a_{n+k-1}(2)^{n+k-1} + \ldots + a_0 \equiv R(2)((2)^k + b_{k-1}(2)^{k-1} \cdots b_0) \pmod{p}$$
$$\vdots$$
$$a_{n+k-1}(m)^{n+k-1} + \ldots + a_0 \equiv R(m)((m)^k + b_{k-1}(m)^{k-1} \cdots b_0) \pmod{p}$$

..and $n+2k$ unknown coefficients of $Q(x)$ and $E(x)$!

Solve for coefficients of $Q(x)$ and $E(x)$.

Find $P(x) = Q(x)/E(x)$. 
Solving for \( Q(x) \) and \( E(x) \)...and \( P(x) \)

For all points \( 1, \ldots, i, n+2k \),

\[
Q(i) = R(i)E(i) \pmod{p}
\]

Gives \( n+2k \) linear equations.

\[
a_{n+k-1} + \ldots a_0 \equiv R(1)(1 + b_{k-1} \cdots b_0) \pmod{p}
\]

\[
a_{n+k-1}(2)^{n+k-1} + \ldots a_0 \equiv R(2)((2)^k + b_{k-1}(2)^{k-1} \cdots b_0) \pmod{p}
\]

\[
\vdots
\]

\[
a_{n+k-1}(m)^{n+k-1} + \ldots a_0 \equiv R(m)((m)^k + b_{k-1}(m)^{k-1} \cdots b_0) \pmod{p}
\]

..and \( n+2k \) unknown coefficients of \( Q(x) \) and \( E(x) \)!

Solve for coefficients of \( Q(x) \) and \( E(x) \).

Find \( P(x) = Q(x)/E(x) \).
Example.

Received $R(1) = 3$, $R(2) = 1$, $R(3) = 6$, $R(4) = 0$, $R(5) = 3$
Example.

Received $R(1) = 3, R(2) = 1, R(3) = 6, R(4) = 0, R(5) = 3$

$Q(x) = E(x)P(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0$
Example.

Received $R(1) = 3, R(2) = 1, R(3) = 6, R(4) = 0, R(5) = 3$

$Q(x) = E(x)P(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0$

$E(x) = x - b_0$
Example.

Received $R(1) = 3, R(2) = 1, R(3) = 6, R(4) = 0, R(5) = 3$

$Q(x) = E(x)P(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0$

$E(x) = x - b_0$

$Q(i) = R(i)E(i)$. 
Example.

Received $R(1) = 3, R(2) = 1, R(3) = 6, R(4) = 0, R(5) = 3$

$Q(x) = E(x)P(x) = a_3x^3 + a_2x^2 + a_1x + a_0$

$E(x) = x - b_0$

$Q(i) = R(i)E(i)$.

$$a_3 + a_2 + a_1 + a_0 \equiv 3(1 - b_0) \pmod{7}$$
Example.

Received $R(1) = 3, R(2) = 1, R(3) = 6, R(4) = 0, R(5) = 3$

$Q(x) = E(x)P(x) = a_3x^3 + a_2x^2 + a_1x + a_0$

$E(x) = x - b_0$

$Q(i) = R(i)E(i)$.

\[
\begin{align*}
    a_3 + a_2 + a_1 + a_0 & \equiv 3(1 - b_0) \pmod{7} \\
    a_3 + 4a_2 + 2a_1 + a_0 & \equiv 1(2 - b_0) \pmod{7}
\end{align*}
\]
Example.

Received $R(1) = 3, R(2) = 1, R(3) = 6, R(4) = 0, R(5) = 3$

$Q(x) = E(x)P(x) = a_3x^3 + a_2x^2 + a_1x + a_0$

$E(x) = x - b_0$

$Q(i) = R(i)E(i)$.

\[
\begin{align*}
    a_3 + a_2 + a_1 + a_0 & \equiv 3(1 - b_0) \pmod{7} \\
    a_3 + 4a_2 + 2a_1 + a_0 & \equiv 1(2 - b_0) \pmod{7} \\
    6a_3 + 2a_2 + 3a_1 + a_0 & \equiv 6(3 - b_0) \pmod{7} \\
    a_3 + 2a_2 + 4a_1 + a_0 & \equiv 0(4 - b_0) \pmod{7} \\
    6a_3 + 4a_2 + 5a_1 + a_0 & \equiv 3(5 - b_0) \pmod{7}
\end{align*}
\]
Example.

Received $R(1) = 3$, $R(2) = 1$, $R(3) = 6$, $R(4) = 0$, $R(5) = 3$

$Q(x) = E(x)P(x) = a_3x^3 + a_2x^2 + a_1x + a_0$

$E(x) = x - b_0$

$Q(i) = R(i)E(i)$.

$$a_3 + a_2 + a_1 + a_0 \equiv 3(1 - b_0) \pmod{7}$$
$$a_3 + 4a_2 + 2a_1 + a_0 \equiv 1(2 - b_0) \pmod{7}$$
$$6a_3 + 2a_2 + 3a_1 + a_0 \equiv 6(3 - b_0) \pmod{7}$$
$$a_3 + 2a_2 + 4a_1 + a_0 \equiv 0(4 - b_0) \pmod{7}$$
$$6a_3 + 4a_2 + 5a_1 + a_0 \equiv 3(5 - b_0) \pmod{7}$$

$a_3 = 1$, $a_2 = 6$, $a_1 = 6$, $a_0 = 5$ and $b_0 = 2$. 
Example.

Received $R(1) = 3, R(2) = 1, R(3) = 6, R(4) = 0, R(5) = 3$

$Q(x) = E(x)P(x) = a_3x^3 + a_2x^2 + a_1x + a_0$

$E(x) = x - b_0$

$Q(i) = R(i)E(i)$.

\[
\begin{align*}
a_3 + a_2 + a_1 + a_0 & \equiv 3(1 - b_0) \pmod{7} \\
a_3 + 4a_2 + 2a_1 + a_0 & \equiv 1(2 - b_0) \pmod{7} \\
6a_3 + 2a_2 + 3a_1 + a_0 & \equiv 6(3 - b_0) \pmod{7} \\
a_3 + 2a_2 + 4a_1 + a_0 & \equiv 0(4 - b_0) \pmod{7} \\
6a_3 + 4a_2 + 5a_1 + a_0 & \equiv 3(5 - b_0) \pmod{7}
\end{align*}
\]

$a_3 = 1, a_2 = 6, a_1 = 6, a_0 = 5$ and $b_0 = 2$.

$Q(x) = x^3 + 6x^2 + 6x + 5$. 
Example.

Received $R(1) = 3$, $R(2) = 1$, $R(3) = 6$, $R(4) = 0$, $R(5) = 3$

$Q(x) = E(x)P(x) = a_3x^3 + a_2x^2 + a_1x + a_0$

$E(x) = x - b_0$

$Q(i) = R(i)E(i)$.

\[
\begin{align*}
  a_3 + a_2 + a_1 + a_0 & \equiv 3(1 - b_0) \pmod{7} \\
  a_3 + 4a_2 + 2a_1 + a_0 & \equiv 1(2 - b_0) \pmod{7} \\
  6a_3 + 2a_2 + 3a_1 + a_0 & \equiv 6(3 - b_0) \pmod{7} \\
  a_3 + 2a_2 + 4a_1 + a_0 & \equiv 0(4 - b_0) \pmod{7} \\
  6a_3 + 4a_2 + 5a_1 + a_0 & \equiv 3(5 - b_0) \pmod{7}
\end{align*}
\]

$a_3 = 1$, $a_2 = 6$, $a_1 = 6$, $a_0 = 5$ and $b_0 = 2$.

$Q(x) = x^3 + 6x^2 + 6x + 5$.

$E(x) = x - 2$. 
Example: finishing up.

\[ Q(x) = x^3 + 6x^2 + 6x + 5. \]
Example: finishing up.

\[ Q(x) = x^3 + 6x^2 + 6x + 5. \]
\[ E(x) = x - 2. \]
Example: finishing up.

\[ Q(x) = x^3 + 6x^2 + 6x + 5. \]
\[ E(x) = x - 2. \]

\[
\begin{array}{c|cccc}
 & x^3 & +6x^2 & +6x & +5 \\
\hline
x - 2 & x^3 & +6x^2 & +6x & +5 \\
 & \hline
 & x^2 & -2x & -5 \\
 & \hline
 & 0 & \\
\end{array}
\]
Example: finishing up.

\[ Q(x) = x^3 + 6x^2 + 6x + 5. \]
\[ E(x) = x - 2. \]

\[
\begin{array}{c}
1 \quad x^2 \\
\hline \\
\end{array}
\]

\[
\begin{array}{c}
x - 2 \\
\hline \\
x^3 + 6x^2 + 6x + 5 \\
x^3 - 2x^2 \\
\hline \\
x + 5 \\
x - 2 \\
0
\end{array}
\]

\[ P(x) = x^2 + x + 1 \]

Message is \[ P(1) = 3, \]
\[ P(2) = 0, \]
\[ P(3) = 6. \]

What is \[ x - 2 \] except at \[ x = 2? \]?
Example: finishing up.

\[ Q(x) = x^3 + 6x^2 + 6x + 5. \]
\[ E(x) = x - 2. \]

\[
\begin{array}{c|cccc}
 & 1 & x^2 & 0 & 0 \\
\hline
x - 2 & ) & x^3 & + & 6x^2 & + & 6x & + & 5 \\
 & x^3 & - & 2x^2 & & & & & \\
\hline
 & 1 & x^2 & + & 6x & + & 5 \\
\end{array}
\]
Example: finishing up.

\[ Q(x) = x^3 + 6x^2 + 6x + 5. \]
\[ E(x) = x - 2. \]

\[
\begin{array}{r}
1 \ x^2 + 1 \ x \\
\hline
x - 2 \ \\
\hline
\end{array}
\]

\[
\begin{array}{r}
x^3 + 6 \ x^2 + 6 \ x + 5 \\
\hline
x^3 - 2 \ x^2 \\
\hline
1 \ x^2 + 6 \ x + 5 \\
\hline
1 \ x^2 - 2 \ x \\
\hline
0
\end{array}
\]

\[ P(x) = x^2 + x + 1 \]

Message is \[ P(1) = 3, \ P(2) = 0, \ P(3) = 6. \]

What is \[ x - 2 \] except at \[ x = 2? \] Hole there?
Example: finishing up.

\[ Q(x) = x^3 + 6x^2 + 6x + 5. \]
\[ E(x) = x - 2. \]

\[
\begin{array}{c}
1 \ x^2 + 1 \ x \\
\hline
x - 2 ) \ x^3 + 6 \ x^2 + 6 \ x + 5 \\
\hline
x^3 - 2 \ x^2 \\
\hline
1 \ x^2 + 6 \ x + 5 \\
\hline
1 \ x^2 - 2 \ x \\
\hline
x + 5
\end{array}
\]
Example: finishing up.

\[ Q(x) = x^3 + 6x^2 + 6x + 5. \]
\[ E(x) = x - 2. \]

\[
\begin{array}{r|llll}
& x^3 & + & 6x^2 & + 6x & + 5 \\
\hline
x - 2 & x^2 & + & 6x & + 5 \\
  & x^2 & - & 2x & \\
\hline
  & 1x^2 & + & 6x & + 5 \\
  & 1x^2 & - & 2x & \\
\hline
  & x & + & 5 \\
  & x & - & 2 \\
\end{array}
\]
Example: finishing up.

\[ Q(x) = x^3 + 6x^2 + 6x + 5. \]
\[ E(x) = x - 2. \]

\[
\begin{array}{cccc}
\text{1} & x^2 & + & 1 \\
\hline
x & - & 2 & ) \ x^3 & + & 6x^2 & + & 6x & + & 5 \\
\hline
& x^3 & - & 2x^2 & & & & & & & \\
\hline
& 1x^2 & + & 6x & + & 5 & & & & & \\
\hline
& 1x^2 & - & 2x & & & & & & & \\
\hline
& x & + & 5 & & & & & & & \\
\hline
& x & - & 2 & & & & & & & \\
\hline
& & & & & & & & 0 & & & \\
\end{array}
\]
Example: finishing up.

\[ Q(x) = x^3 + 6x^2 + 6x + 5. \]
\[ E(x) = x - 2. \]

\[
\begin{array}{r}
1 \ x^2 + 1 \ x + 1 \\
\hline
x - 2 \\
\end{array}
\]

\[
\begin{array}{r}
x^3 + 6x^2 + 6x + 5 \\
x^3 - 2x^2 \\
\hline
1x^2 + 6x + 5 \\
1x^2 - 2x \\
\hline
x + 5 \\
x - 2 \\
\hline
0
\end{array}
\]

\[ P(x) = x^2 + x + 1 \]
Example: finishing up.

\[ Q(x) = x^3 + 6x^2 + 6x + 5. \]
\[ E(x) = x - 2. \]

\[
\begin{array}{c}
1 \ x^2 + 1 \ x + 1 \\
\hline
x - 2 ) \ x^3 + 6 \ x^2 + 6 \ x + 5 \\
\hline
x^3 - 2 \ x^2 \\
\hline
1 \ x^2 + 6 \ x + 5 \\
\hline
1 \ x^2 - 2 \ x \\
\hline
x + 5 \\
\hline
x - 2 \\
\hline
0
\end{array}
\]

\[ P(x) = x^2 + x + 1 \]
Message is \( P(1) = 3, P(2) = 0, P(3) = 6. \)
Example: finishing up.

\[ Q(x) = x^3 + 6x^2 + 6x + 5. \]
\[ E(x) = x - 2. \]

\[
\begin{array}{r}
1 & x^2 & + & 1 & x & + & 1 \\
\hline
x - 2 & ) & x^3 & + & 6x^2 & + & 6x & + & 5 \\
\hline
x^3 & - & 2x^2 & & & & & & \\
\hline
1 & x^2 & + & 6x & + & 5 \\
1 & x^2 & - & 2x & & & & & \\
\hline
x & + & 5 \\
x & - & 2 \\
\hline
0 \\
\end{array}
\]

\[ P(x) = x^2 + x + 1 \]
Message is \( P(1) = 3, P(2) = 0, P(3) = 6. \)

What is \( \frac{x-2}{x-2} \)?
Example: finishing up.

\[ Q(x) = x^3 + 6x^2 + 6x + 5. \]
\[ E(x) = x - 2. \]

\[
\begin{array}{r}
1 \ x^2 + 1 \ x + 1 \\
\hline
\end{array}
\]

\[
\begin{array}{r}
x - 2 \ ) \ x^3 + 6x^2 + 6x + 5 \\
\hline
x^3 - 2x^2 \\
\hline
1 \ x^2 + 6 \ x + 5 \\
\hline
1 \ x^2 - 2 \ x \\
\hline
x + 5 \\
\hline
x - 2 \\
\hline
0
\end{array}
\]

\[ P(x) = x^2 + x + 1 \]
Message is \( P(1) = 3, P(2) = 0, P(3) = 6. \)

What is \( \frac{x - 2}{x - 2} \)? 1   Except at \( x = 2 \)?
Example: finishing up.

\[ Q(x) = x^3 + 6x^2 + 6x + 5. \]
\[ E(x) = x - 2. \]

\[
\begin{array}{c}
  \begin{array}{c}
    1 \ x^2 + 1 \ x + 1 \\
    \hline
    x - 2 \\
    \end{array}
  \\
  \begin{array}{c}
    x^3 + 6x^2 + 6x + 5 \\
   x^3 - 2x^2 \\
   \hline
   1 \ x^2 + 6x + 5 \\
   1 \ x^2 - 2x \\
\end{array}
  \\
  \begin{array}{c}
    \hline
    x + 5 \\
    x - 2 \\
\end{array}
  \\
  \hline
  0
\end{array}
\]

\[ P(x) = x^2 + x + 1 \]
Message is \( P(1) = 3, P(2) = 0, P(3) = 6. \)

What is \( \frac{x-2}{x-2} \)? 1  
Except at \( x = 2? \) Hole there?
Error Correction: Berlekamp-Welsh

Message: $m_1, \ldots, m_n$.

Sender:
1. Form degree $n-1$ polynomial $P(x)$ where $P(i) = m_i$.
2. Send $P(1), \ldots, P(n+2k)$.

Receiver:
1. Receive $R(1), \ldots, R(n+2k)$.
2. Solve $n+2k$ equations, $Q(i) = E(i) R(i)$ to find $Q(x) = E(x) P(x)$ and $E(x)$.
3. Compute $P(x) = Q(x) / E(x)$.
4. Compute $P(1), \ldots, P(n)$.
Check your understanding.

You have error locator polynomial!
Check your understanding.

You have error locator polynomial!
Where oh where can my bad packets be?...
Check your understanding.

You have error locator polynomial!
Where oh where can my bad packets be?...
Factor?
Check your understanding.

You have error locator polynomial!
Where oh where can my bad packets be?...
Factor? Sure.
Check your understanding.

You have error locator polynomial!

Where oh where can my **bad** packets be?...

Factor? Sure.
Check all values?
Check your understanding.

You have error locator polynomial!
Where oh where can my bad packets be?...
Factor? Sure.
Check all values? Sure.
Check your understanding.

You have error locator polynomial!
Where oh where can my **bad** packets be?...
Factor? Sure.
Check all values? Sure.
Check your understanding.

You have error locator polynomial!
Where oh where can my bad packets be?...
Factor? Sure.
Check all values? Sure.
Efficiency?
Check your understanding.

You have error locator polynomial!
Where oh where can my **bad** packets be?...
Factor? Sure.
Check all values? Sure.
Efficiency? Sure.
You have error locator polynomial!

Where oh where can my **bad** packets be?...

Factor? Sure.
Check all values? Sure.

Efficiency? Sure. Only $n + k$ values.
Check your understanding.

You have error locator polynomial!
Where oh where can my **bad** packets be?...
Factor? Sure.
Check all values? Sure.
Efficiency? Sure. Only $n + k$ values.
See where it is 0.
Hmmm...

Is there one and only one $P(x)$ from Berlekamp-Welsh procedure?
Is there one and only one $P(x)$ from Berlekamp-Welsh procedure?

Existence: there is a $P(x)$ and $E(x)$ that satisfy equations.
Unique solution for $P(x)$

**Uniqueness:** any solution $Q'(x)$ and $E'(x)$ have

$$\frac{Q'(x)}{E'(x)} = \frac{Q(x)}{E(x)} = P(x).$$  \hspace{1cm} (1)
Unique solution for $P(x)$

**Uniqueness**: any solution $Q'(x)$ and $E'(x)$ have

$$\frac{Q'(x)}{E'(x)} = \frac{Q(x)}{E(x)} = P(x).$$

(1)

**Proof:**

Equation 2 implies 1: $Q'(x)$ and $E'(x)$ agree on $n + 2k$ points.
Unique solution for $P(x)$

**Uniqueness:** any solution $Q'(x)$ and $E'(x)$ have

$$\frac{Q'(x)}{E'(x)} = \frac{Q(x)}{E(x)} = P(x).$$

(1)

**Proof:**

We claim
Unique solution for $P(x)$

**Uniqueness:** any solution $Q'(x)$ and $E'(x)$ have

\[
\frac{Q'(x)}{E'(x)} = \frac{Q(x)}{E(x)} = P(x).
\]  

(1)

**Proof:**

We claim

\[Q'(x)E(x) = Q(x)E'(x) \text{ on } n+2k \text{ values of } x.\]  

(2)
Unique solution for $P(x)$

**Uniqueness:** any solution $Q'(x)$ and $E'(x)$ have

$$\frac{Q'(x)}{E'(x)} = \frac{Q(x)}{E(x)} = P(x).$$

**Proof:**
We claim

$$Q'(x)E(x) = Q(x)E'(x) \text{ on } n+2k \text{ values of } x.$$  

(2)

Equation 2 implies 1:
Unique solution for \( P(x) \)

**Uniqueness:** any solution \( Q'(x) \) and \( E'(x) \) have

\[
\frac{Q'(x)}{E'(x)} = \frac{Q(x)}{E(x)} = P(x) \tag{1}
\]

**Proof:**
We claim

\[
Q'(x)E(x) = Q(x)E'(x) \text{ on } n + 2k \text{ values of } x. \tag{2}
\]

Equation 2 implies 1:

\( Q'(x)E(x) \) and \( Q(x)E'(x) \) are degree \( n + 2k - 1 \).
**Unique solution for** $P(x)$

**Uniqueness:** any solution $Q'(x)$ and $E'(x)$ have

$$\frac{Q'(x)}{E'(x)} = \frac{Q(x)}{E(x)} = P(x).$$ \quad (1)

**Proof:**
We claim

$$Q'(x)E(x) = Q(x)E'(x) \text{ on } n + 2k \text{ values of } x. \quad (2)$$

Equation 2 implies 1:

$Q'(x)E(x)$ and $Q(x)E'(x)$ are degree $n + 2k - 1$
and agree on $n + 2k$ points

Unique solution for \( P(x) \)

**Uniqueness:** any solution \( Q'(x) \) and \( E'(x) \) have

\[
\frac{Q'(x)}{E'(x)} = \frac{Q(x)}{E(x)} = P(x).
\]  

(1)

**Proof:**

We claim

\[
Q'(x)E(x) = Q(x)E'(x) \text{ on } n + 2k \text{ values of } x.
\]

(2)

Equation 2 implies 1:

\( Q'(x)E(x) \) and \( Q(x)E'(x) \) are degree \( n + 2k - 1 \)

and agree on \( n + 2k \) points

\( E(x) \) and \( E'(x) \) have at most \( k \) zeros each.
Unique solution for $P(x)$

**Uniqueness:** any solution $Q'(x)$ and $E'(x)$ have

$$\frac{Q'(x)}{E'(x)} = \frac{Q(x)}{E(x)} = P(x).$$  \hspace{1cm} (1)

**Proof:**
We claim

$$Q'(x)E(x) = Q(x)E'(x) \text{ on } n+2k \text{ values of } x. \hspace{1cm} (2)$$

Equation 2 implies 1:

$Q'(x)E(x)$ and $Q(x)E'(x)$ are degree $n+2k-1$

and agree on $n+2k$ points

$E(x)$ and $E'(x)$ have at most $k$ zeros each.

Can cross divide at $n$ points.
Unique solution for $P(x)$

**Uniqueness:** any solution $Q'(x)$ and $E'(x)$ have

\[
\frac{Q'(x)}{E'(x)} = \frac{Q(x)}{E(x)} = P(x).
\]  
\[
(1)
\]

**Proof:**
We claim

\[
Q'(x)E(x) = Q(x)E'(x) \text{ on } n+2k \text{ values of } x.
\]  
\[
(2)
\]

Equation 2 implies 1:

$Q'(x)E(x)$ and $Q(x)E'(x)$ are degree $n+2k-1$

and agree on $n+2k$ points

$E(x)$ and $E'(x)$ have at most $k$ zeros each.

Can cross divide at $n$ points.

\[
\Longrightarrow \frac{Q'(x)}{E'(x)} = \frac{Q(x)}{E(x)} \text{ equal on } n \text{ points.}
\]
Unique solution for $P(x)$

**Uniqueness:** any solution $Q'(x)$ and $E'(x)$ have

$$\frac{Q'(x)}{E'(x)} = \frac{Q(x)}{E(x)} = P(x). \quad (1)$$

**Proof:**

We claim

$$Q'(x)E(x) = Q(x)E'(x) \text{ on } n+2k \text{ values of } x. \quad (2)$$

Equation 2 implies 1:

$Q'(x)E(x)$ and $Q(x)E'(x)$ are degree $n+2k-1$

and agree on $n+2k$ points

$E(x)$ and $E'(x)$ have at most $k$ zeros each.

Can cross divide at $n$ points.

$$\implies \frac{Q'(x)}{E'(x)} = \frac{Q(x)}{E(x)} \text{ equal on } n \text{ points.}$$

Both degree $\leq n$
Unique solution for $P(x)$

**Uniqueness:** any solution $Q'(x)$ and $E'(x)$ have

$$\frac{Q'(x)}{E'(x)} = \frac{Q(x)}{E(x)} = P(x). \quad (1)$$

**Proof:**

We claim

$$Q'(x)E(x) = Q(x)E'(x) \text{ on } n+2k \text{ values of } x. \quad (2)$$

Equation 2 implies 1:

$Q'(x)E(x)$ and $Q(x)E'(x)$ are degree $n+2k-1$

and agree on $n+2k$ points

$E(x)$ and $E'(x)$ have at most $k$ zeros each.

Can cross divide at $n$ points.

$$\implies \frac{Q'(x)}{E'(x)} = \frac{Q(x)}{E(x)} \text{ equal on } n \text{ points.}$$

Both degree $\leq n \implies$ Same polynomial!
Unique solution for $P(x)$

**Uniqueness:** any solution $Q'(x)$ and $E'(x)$ have

$$\frac{Q'(x)}{E'(x)} = \frac{Q(x)}{E(x)} = P(x).$$  \hspace{1cm} (1)

**Proof:**

We claim

$$Q'(x)E(x) = Q(x)E'(x) \text{ on } n + 2k \text{ values of } x.$$ \hspace{1cm} (2)

Equation 2 implies 1:

$Q'(x)E(x)$ and $Q(x)E'(x)$ are degree $n + 2k - 1$
and agree on $n + 2k$ points
$E(x)$ and $E'(x)$ have at most $k$ zeros each.
Can cross divide at $n$ points.

$$\implies \frac{Q'(x)}{E'(x)} = \frac{Q(x)}{E(x)} \text{ equal on } n \text{ points}.$$  
Both degree $\leq n \implies$ Same polynomial!
Fact: $Q'(x)E(x) = Q(x)E'(x)$ on $n + 2k$ values of $x$. 

Last bit.
Last bit.

Fact: $Q'(x)E(x) = Q(x)E'(x)$ on $n + 2k$ values of $x$.

Proof:
Fact: $Q'(x)E(x) = Q(x)E'(x)$ on $n + 2k$ values of $x$.

Proof: Construction implies that
Last bit.

**Fact:** $Q'(x)E(x) = Q(x)E'(x)$ on $n + 2k$ values of $x$.

**Proof:** Construction implies that

$$Q(i) = R(i)E(i)$$

$$Q'(i) = R(i)E'(i)$$
Fact: \( Q'(x)E(x) = Q(x)E'(x) \) on \( n + 2k \) values of \( x \).

Proof: Construction implies that

\[
Q(i) = R(i)E(i) \\
Q'(i) = R(i)E'(i)
\]

for \( i \in \{1, \ldots n + 2k\} \).
Fact: \( Q'(x)E(x) = Q(x)E'(x) \) on \( n+2k \) values of \( x \).

Proof: Construction implies that

\[
Q(i) = R(i)E(i) \\
Q'(i) = R(i)E'(i)
\]

for \( i \in \{1, \ldots n+2k\} \).

If \( E(i) = 0 \), then \( Q(i) = 0 \).
Fact: \( Q'(x)E(x) = Q(x)E'(x) \) on \( n + 2k \) values of \( x \).

Proof: Construction implies that

\[
Q(i) = R(i)E(i) \\
Q'(i) = R(i)E'(i)
\]

for \( i \in \{1, \ldots n + 2k\} \).

If \( E(i) = 0 \), then \( Q(i) = 0 \). If \( E'(i) = 0 \), then \( Q'(i) = 0 \).
Fact: $Q'(x)E(x) = Q(x)E'(x)$ on $n + 2k$ values of $x$.

Proof: Construction implies that

$$Q(i) = R(i)E(i)$$
$$Q'(i) = R(i)E'(i)$$

for $i \in \{1, \ldots n + 2k\}$.

If $E(i) = 0$, then $Q(i) = 0$. If $E'(i) = 0$, then $Q'(i) = 0$.

$$\implies Q(i)E'(i) = Q'(i)E(i)$$

holds when $E(i)$ or $E'(i)$ are zero.
Fact: $Q'(x)E(x) = Q(x)E'(x)$ on $n + 2k$ values of $x$.

Proof: Construction implies that

$$Q(i) = R(i)E(i)$$
$$Q'(i) = R(i)E'(i)$$

for $i \in \{1, \ldots n + 2k\}$.

If $E(i) = 0$, then $Q(i) = 0$. If $E'(i) = 0$, then $Q'(i) = 0$.

$$\implies Q(i)E'(i) = Q'(i)E(i)$$
holds when $E(i)$ or $E'(i)$ are zero.

When $E'(i)$ and $E(i)$ are not zero
Fact: \( Q'(x)E(x) = Q(x)E'(x) \) on \( n+2k \) values of \( x \).

Proof: Construction implies that

\[
Q(i) = R(i)E(i)
\]
\[
Q'(i) = R(i)E'(i)
\]
or \( i \in \{1, \ldots n+2k\} \).

If \( E(i) = 0 \), then \( Q(i) = 0 \). If \( E'(i) = 0 \), then \( Q'(i) = 0 \).

\( \implies \) \( Q(i)E'(i) = Q'(i)E(i) \) holds when \( E(i) \) or \( E'(i) \) are zero.

When \( E'(i) \) and \( E(i) \) are not zero

\[
\frac{Q'(i)}{E'(i)} = \frac{Q(i)}{E(i)} = R(i).
\]
Fact: \( Q'(x)E(x) = Q(x)E'(x) \) on \( n+2k \) values of \( x \).

Proof: Construction implies that

\[
Q(i) = R(i)E(i) \\
Q'(i) = R(i)E'(i)
\]

for \( i \in \{1, \ldots n+2k\} \).

If \( E(i) = 0 \), then \( Q(i) = 0 \). If \( E'(i) = 0 \), then \( Q'(i) = 0 \).

\[
\implies Q(i)E'(i) = Q'(i)E(i) \text{ holds when } E(i) \text{ or } E'(i) \text{ are zero.}
\]

When \( E'(i) \) and \( E(i) \) are not zero

\[
\frac{Q'(i)}{E'(i)} = \frac{Q(i)}{E(i)} = R(i).
\]

Cross multiplying gives equality in fact for these points.
Fact: $Q'(x)E(x) = Q(x)E'(x)$ on $n + 2k$ values of $x$.

Proof: Construction implies that

$$Q(i) = R(i)E(i)$$
$$Q'(i) = R(i)E'(i)$$

for $i \in \{1, \ldots n + 2k\}$.

If $E(i) = 0$, then $Q(i) = 0$. If $E'(i) = 0$, then $Q'(i) = 0$.  
$$\implies Q(i)E'(i) = Q'(i)E(i)$$ holds when $E(i)$ or $E'(i)$ are zero.

When $E'(i)$ and $E(i)$ are not zero

$$\frac{Q'(i)}{E'(i)} = \frac{Q(i)}{E(i)} = R(i).$$

Cross multiplying gives equality in fact for these points.  \qed
Fact: \( Q'(x)E(x) = Q(x)E'(x) \) on \( n + 2k \) values of \( x \).

Proof: Construction implies that

\[
Q(i) = R(i)E(i) \\
Q'(i) = R(i)E'(i)
\]

for \( i \in \{1, \ldots n + 2k\} \).

If \( E(i) = 0 \), then \( Q(i) = 0 \). If \( E'(i) = 0 \), then \( Q'(i) = 0 \).

\[
\implies Q(i)E'(i) = Q'(i)E(i)
\]

holds when \( E(i) \) or \( E'(i) \) are zero.

When \( E'(i) \) and \( E(i) \) are not zero

\[
\frac{Q'(i)}{E'(i)} = \frac{Q(i)}{E(i)} = R(i).
\]

Cross multiplying gives equality in fact for these points.

Points to polynomials, have to deal with zeros!
Fact: $Q'(x)E(x) = Q(x)E'(x)$ on $n + 2k$ values of $x$.

Proof: Construction implies that

$$Q(i) = R(i)E(i)$$
$$Q'(i) = R(i)E'(i)$$

for $i \in \{1, \ldots n + 2k\}$.

If $E(i) = 0$, then $Q(i) = 0$. If $E'(i) = 0$, then $Q'(i) = 0$.

$$\implies Q(i)E'(i) = Q'(i)E(i)$$

holds when $E(i)$ or $E'(i)$ are zero.

When $E'(i)$ and $E(i)$ are not zero

$$\frac{Q'(i)}{E'(i)} = \frac{Q(i)}{E(i)} = R(i).$$

Cross multiplying gives equality in fact for these points.

Points to polynomials, have to deal with zeros!

Example: dealing with $\frac{x-2}{x-2}$ at $x = 2$. 
Berlekamp-Welsh algorithm decodes correctly when $k$ errors!
Summary: polynomials.

Set of $d + 1$ points determines degree $d$ polynomial.
Summary: polynomials.

Set of $d + 1$ points determines degree $d$ polynomial.

Encode secret using degree $k - 1$ polynomial:
Summary: polynomials.

Set of $d + 1$ points determines degree $d$ polynomial.

Encode secret using degree $k - 1$ polynomial:
   Can share with $n$ people.
Summary: polynomials.

Set of $d+1$ points determines degree $d$ polynomial.

Encode secret using degree $k-1$ polynomial:
  Can share with $n$ people. Any $k$ can recover!
Summary: polynomials.

Set of $d + 1$ points determines degree $d$ polynomial.

Encode secret using degree $k - 1$ polynomial:
   Can share with $n$ people. Any $k$ can recover!

Encode message using degree $n - 1$ polynomial:
Summary: polynomials.

Set of $d + 1$ points determines degree $d$ polynomial.

Encode secret using degree $k - 1$ polynomial:
  Can share with $n$ people. Any $k$ can recover!

Encode message using degree $n - 1$ polynomial:
  $n$ packets of information.
Summary: polynomials.

Set of $d + 1$ points determines degree $d$ polynomial.

Encode secret using degree $k - 1$ polynomial:
   Can share with $n$ people. Any $k$ can recover!

Encode message using degree $n - 1$ polynomial:
   $n$ packets of information.

Send $n + k$ packets (point values).
Summary: polynomials.

Set of $d + 1$ points determines degree $d$ polynomial.

Encode secret using degree $k - 1$ polynomial:
Can share with $n$ people. Any $k$ can recover!

Encode message using degree $n - 1$ polynomial:
$n$ packets of information.

Send $n + k$ packets (point values).
Can recover from $k$ losses:
Summary: polynomials.

Set of $d + 1$ points determines degree $d$ polynomial.

Encode secret using degree $k - 1$ polynomial:
  - Can share with $n$ people. Any $k$ can recover!

Encode message using degree $n - 1$ polynomial:
  - $n$ packets of information.

Send $n + k$ packets (point values).
  - Can recover from $k$ losses: Still have $n$ points!
Summary: polynomials.

Set of $d + 1$ points determines degree $d$ polynomial.

Encode secret using degree $k - 1$ polynomial:
  Can share with $n$ people. Any $k$ can recover!

Encode message using degree $n - 1$ polynomial:
  $n$ packets of information.

Send $n + k$ packets (point values).
  Can recover from $k$ losses: Still have $n$ points!

Send $n + 2k$ packets (point values).
Summary: polynomials.

Set of $d + 1$ points determines degree $d$ polynomial.

Encode secret using degree $k - 1$ polynomial:
  Can share with $n$ people. Any $k$ can recover!

Encode message using degree $n - 1$ polynomial:
  $n$ packets of information.

Send $n + k$ packets (point values).
  Can recover from $k$ losses: Still have $n$ points!

Send $n + 2k$ packets (point values).
  Can recover from $k$ corruptionss.
Summary: polynomials.

Set of \( d + 1 \) points determines degree \( d \) polynomial.

Encode secret using degree \( k - 1 \) polynomial:
   Can share with \( n \) people. Any \( k \) can recover!

Encode message using degree \( n - 1 \) polynomial:
   \( n \) packets of information.

Send \( n + k \) packets (point values).
   Can recover from \( k \) losses: Still have \( n \) points!

Send \( n + 2k \) packets (point values).
   Can recover from \( k \) corruptionss.
   Only one polynomial contains \( n + k \)

Efficiency.

Magic!!!!

Magic of polynomials.

Other Algebraic-Geometric codes.
Summary: polynomials.

Set of $d + 1$ points determines degree $d$ polynomial.

Encode secret using degree $k - 1$ polynomial:
   Can share with $n$ people. Any $k$ can recover!

Encode message using degree $n - 1$ polynomial:
   $n$ packets of information.

Send $n + k$ packets (point values).
   Can recover from $k$ losses: Still have $n$ points!

Send $n + 2k$ packets (point values).
   Can recover from $k$ corruptions.
      Only one polynomial contains $n + k$

Efficiency.
Summary: polynomials.

Set of $d + 1$ points determines degree $d$ polynomial.

Encode secret using degree $k - 1$ polynomial:
   Can share with $n$ people. Any $k$ can recover!

Encode message using degree $n - 1$ polynomial:
   $n$ packets of information.

Send $n + k$ packets (point values).
   Can recover from $k$ losses: Still have $n$ points!

Send $n + 2k$ packets (point values).
   Can recover from $k$ corruptionss.
      Only one polynomial contains $n + k$
   Efficiency.
      Magic!!!!
Summary: polynomials.

Set of $d + 1$ points determines degree $d$ polynomial.

Encode secret using degree $k - 1$ polynomial:
  Can share with $n$ people. Any $k$ can recover!

Encode message using degree $n - 1$ polynomial:
  $n$ packets of information.

Send $n + k$ packets (point values).
  Can recover from $k$ losses: Still have $n$ points!

Send $n + 2k$ packets (point values).
  Can recover from $k$ corruptionss.
    Only one polynomial contains $n + k$

Efficiency.
  Magic!!!!
  Error Locator Polynomial.
Summary: polynomials.

Set of $d + 1$ points determines degree $d$ polynomial.

Encode secret using degree $k - 1$ polynomial:
  Can share with $n$ people. Any $k$ can recover!

Encode message using degree $n - 1$ polynomial:
  $n$ packets of information.

Send $n + k$ packets (point values).
  Can recover from $k$ losses: Still have $n$ points!

Send $n + 2k$ packets (point values).
  Can recover from $k$ corruptionss.
  Only one polynomial contains $n + k$

Efficiency.
  Magic!!!!
  Error Locator Polynomial.

Relations:
Summary: polynomials.

*Set of $d + 1$ points determines degree $d$ polynomial.*

Encode secret using degree $k - 1$ polynomial:
  - Can share with $n$ people. Any $k$ can recover!

Encode message using degree $n - 1$ polynomial:
  - $n$ packets of information.

Send $n + k$ packets (point values).
  - Can recover from $k$ losses: Still have $n$ points!

Send $n + 2k$ packets (point values).
  - Can recover from $k$ corrupted points.
    - Only one polynomial contains $n + k$

Efficiency.
  - Magic!!!!
  - Error Locator Polynomial.

Relations:
  - Linear code.
Summary: polynomials.

Set of $d + 1$ points determines degree $d$ polynomial.

Encode secret using degree $k - 1$ polynomial:
   Can share with $n$ people. Any $k$ can recover!

Encode message using degree $n - 1$ polynomial:
   $n$ packets of information.

Send $n + k$ packets (point values).
   Can recover from $k$ losses: Still have $n$ points!

Send $n + 2k$ packets (point values).
   Can recover from $k$ corruptions.
   Only one polynomial contains $n + k$

Efficiency.
   Magic!!!!
   Error Locator Polynomial.

Relations:
   Linear code.
   Almost any coding matrix works.
Summary: polynomials.

Set of $d + 1$ points determines degree $d$ polynomial.

Encode secret using degree $k - 1$ polynomial:
  Can share with $n$ people. Any $k$ can recover!

Encode message using degree $n - 1$ polynomial:
  $n$ packets of information.

Send $n + k$ packets (point values).
  Can recover from $k$ losses: Still have $n$ points!

Send $n + 2k$ packets (point values).
  Can recover from $k$ corruptionss.
    Only one polynomial contains $n + k$

Efficiency.
  Magic!!!!
  Error Locator Polynomial.

Relations:
  Linear code.
    Almost any coding matrix works.
  Vandermonde matrix (the one for Reed-Solomon)..
Summary: polynomials.

Set of $d + 1$ points determines degree $d$ polynomial.

Encode secret using degree $k - 1$ polynomial:
  Can share with $n$ people. Any $k$ can recover!

Encode message using degree $n - 1$ polynomial:
  $n$ packets of information.

Send $n + k$ packets (point values).
  Can recover from $k$ losses: Still have $n$ points!

Send $n + 2k$ packets (point values).
  Can recover from $k$ corruptionss.
    Only one polynomial contains $n + k$

Efficiency.
  Magic!!!!
  Error Locator Polynomial.

Relations:
  Linear code.
  Almost any coding matrix works.
  Vandermonde matrix (the one for Reed-Solomon)..
  allows for efficiency.
Summary: polynomials.

Set of \( d + 1 \) points determines degree \( d \) polynomial.

Encode secret using degree \( k - 1 \) polynomial:
  Can share with \( n \) people. Any \( k \) can recover!

Encode message using degree \( n - 1 \) polynomial:
  \( n \) packets of information.

Send \( n + k \) packets (point values).
  Can recover from \( k \) losses: Still have \( n \) points!

Send \( n + 2k \) packets (point values).
  Can recover from \( k \) corruptionss.
    Only one polynomial contains \( n + k \)
Efficiency.
  Magic!!!!
  Error Locator Polynomial.

Relations:
  Linear code.
  Almost any coding matrix works.
  Vandermonde matrix (the one for Reed-Solomon). ..
    allows for efficiency. Magic of polynomials.
Summary: polynomials.

Set of $d + 1$ points determines degree $d$ polynomial.

Encode secret using degree $k - 1$ polynomial:
  Can share with $n$ people. Any $k$ can recover!

Encode message using degree $n - 1$ polynomial:
  $n$ packets of information.

Send $n + k$ packets (point values).
  Can recover from $k$ losses: Still have $n$ points!

Send $n + 2k$ packets (point values).
  Can recover from $k$ corruptionss.
  Only one polynomial contains $n + k$

Efficiency.
  Magic!!!!
  Error Locator Polynomial.

Relations:
  Linear code.
  Almost any coding matrix works.
  Vandermonde matrix (the one for Reed-Solomon)...
  allows for efficiency. Magic of polynomials.
  Other Algebraic-Geometric codes.
Farewell to modular arithmetic...

   Modular arithmetic modulo a prime.
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative,
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

- Add, subtract, commutative, associative, inverses!
- Allow for solving linear systems, discussing polynomials...

Yes!

\[ 4 \equiv 3 \pmod{7} \]

Yes...

Maybe?

\[ -3 \equiv 3 \pmod{7} \]

Uh oh...

\[ -3 = 4 \pmod{7} \]

Another problem.

4 is close to 3.

But can you get closer?

Sure.

3.5.

Closer.

Sure?

3.25, 3.1, 3.000001...

For real numbers we have the notion of limit, continuity, and derivative...

...and Calculus.

For modular arithmetic...

no Calculus.

Sad face!
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!
Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.
   Add, subtract, commutative, associative, inverses!
   Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?
4 \succ 3 ~?
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!
Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?

4 > 3 ? Yes!
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!
Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?

$4 > 3$ ? Yes!
$4 > 3 \pmod{7}$?
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.
  Add, subtract, commutative, associative, inverses!
  Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?

4 \geq 3 \ ? \ Yes!

4 \geq 3 \ (\text{mod} \ 7) \ ? \ Yes...
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!
Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?

4 \succ 3 \, ? \, Yes!

4 \succ 3 \, (\text{mod} \, 7)\, ? \, Yes...maybe?
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!
Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?

\[ 4 > 3 \] Yes!

\[ 4 > 3 \text{ (mod 7)} \] Yes...maybe?

\[ -3 > 3 \text{ (mod 7)} \]
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!

Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?

4 > 3 ? Yes!

4 > 3 (mod 7)? Yes...maybe?

−3 > 3 (mod 7)? Uh oh..
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!
Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?

$4 > 3$ ? Yes!

$4 > 3 \ (\text{mod } 7)$? Yes...maybe?

$-3 > 3 \ (\text{mod } 7)$? Uh oh.. $-3 = 4 \ (\text{mod } 7)$. 
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.
   Add, subtract, commutative, associative, inverses!
   Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?
4 > 3 ? Yes!
4 > 3 (mod 7)? Yes...maybe?
−3 > 3 (mod 7)? Uh oh.. −3 = 4 (mod 7).

Another problem.
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!
Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?

$4 > 3$ ? Yes!

$4 > 3 \pmod{7}$? Yes...maybe?

$-3 > 3 \pmod{7}$? Uh oh.. $-3 = 4 \pmod{7}$.

Another problem.
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!
Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?

$4 > 3$? Yes!

$4 > 3 \pmod{7}$? Yes...maybe?

$-3 > 3 \pmod{7}$? Uh oh.. $-3 = 4 \pmod{7}$.

Another problem.

4 is close to 3.
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.
Add, subtract, commutative, associative, inverses!
Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?
4 > 3 ? Yes!
4 > 3 (mod 7)? Yes...maybe?
−3 > 3 (mod 7)? Uh oh.. −3 = 4 (mod 7).

Another problem.
4 is close to 3.
But can you get closer?
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!
Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?

$4 \not> 3$? Yes!

$4 \not> 3 \pmod{7}$? Yes...maybe?

$-3 \not> 3 \pmod{7}$? Uh oh.. $-3 = 4 \pmod{7}$.

Another problem.

4 is close to 3.
But can you get closer? Sure.
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!
Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?

4 \succ 3 \ ? \ Yes!

4 \succ 3 \ \text{(mod 7)}? \ Yes...maybe?

−3 \succ 3 \ \text{(mod 7)}? \ Uh \ oh.. \ −3 = 4 \ \text{(mod 7)}.

Another problem.

4 is close to 3.
But can you get closer? Sure. 3.5.
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!
Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?

$4 > 3$ ? Yes!
$4 > 3 \pmod{7}$? Yes...maybe?
$-3 > 3 \pmod{7}$? Uh oh.. $-3 = 4 \pmod{7}$.

Another problem.

4 is close to 3.
But can you get closer? Sure. 3.5. Closer.
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!
Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?

$4 > 3$ ? Yes!

$4 > 3 \pmod{7}$? Yes...maybe?

$-3 > 3 \pmod{7}$? Uh oh.. $-3 = 4 \pmod{7}$.

Another problem.

4 is close to 3.
But can you get closer? Sure. 3.5. Closer. Sure?
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!
Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?

\[ 4 > 3 \ ? \text{ Yes!} \]

\[ 4 > 3 \ (\text{mod } 7)\ ? \text{ Yes...maybe?} \]

\[ -3 > 3 \ (\text{mod } 7)\ ? \text{ Uh oh.. } -3 = 4 \ (\text{mod } 7). \]

Another problem.

4 is close to 3.
But can you get closer? Sure. 3.5. Closer. Sure? 3.25,
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!
Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?

4 > 3? Yes!
4 > 3 (mod 7)? Yes...maybe?
−3 > 3 (mod 7)? Uh oh.. −3 = 4 (mod 7).

Another problem.

4 is close to 3.
But can you get closer? Sure. 3.5. Closer. Sure? 3.25, 3.1,
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!
Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?

4 > 3? Yes!

4 > 3 (mod 7)? Yes...maybe?

−3 > 3 (mod 7)? Uh oh.. −3 = 4 (mod 7).

Another problem.

4 is close to 3.
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!
Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?

\[ 4 > 3 \] ? Yes!

\[ 4 > 3 \pmod{7} \] ? Yes...maybe?

\[ -3 > 3 \pmod{7} \] ? Uh oh.. \[ -3 = 4 \pmod{7} \].

Another problem.

4 is close to 3.
But can you get closer? Sure. 3.5. Closer. Sure? 3.25, 3.1, 3.000001. …
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!
Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?

4 > 3 ? Yes!
4 > 3 (mod 7)? Yes...maybe?
−3 > 3 (mod 7)? Uh oh.. −3 = 4 (mod 7).

Another problem.

4 is close to 3.
But can you get closer? Sure. 3.5. Closer. Sure? 3.25, 3.1, 3.000001. ...

For reals numbers we have the notion of limit, continuity,
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!
Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?

4 > 3? Yes!

4 > 3 (mod 7)? Yes...maybe?

−3 > 3 (mod 7)? Uh oh.. −3 = 4 (mod 7).

Another problem.

4 is close to 3.

For reals numbers we have the notion of limit, continuity, and derivative........
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!
Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?

4 > 3? Yes!

4 > 3 (mod 7)? Yes...maybe?

−3 > 3 (mod 7)? Uh oh.. −3 = 4 (mod 7).

Another problem.

4 is close to 3.
But can you get closer? Sure. 3.5. Closer. Sure? 3.25, 3.1, 3.000001. ... 

For reals numbers we have the notion of limit, continuity, and derivative....... 

....and Calculus.
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.
   Add, subtract, commutative, associative, inverses!
   Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?
   $4 > 3$ ? Yes!
   $4 > 3 \pmod{7}$? Yes...maybe?
   $-3 > 3 \pmod{7}$? Uh oh.. $-3 = 4 \pmod{7}$.

Another problem.

4 is close to 3.
But can you get closer? Sure. 3.5. Closer. Sure? 3.25, 3.1, 3.000001. ....

For reals numbers we have the notion of limit, continuity, and derivative.......

....and Calculus.

For modular arithmetic...
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!
Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?

\[ 4 > 3 \text{? Yes!} \]
\[ 4 > 3 \pmod{7}? \text{Yes...maybe?} \]
\[ -3 > 3 \pmod{7}? \text{Uh oh.. } -3 = 4 \pmod{7}. \]

Another problem.

4 is close to 3.
But can you get closer? Sure. 3.5. Closer. Sure? 3.25, 3.1, 3.000001. ... 

For reals numbers we have the notion of limit, continuity, and derivative......

....and Calculus.

For modular arithmetic...no Calculus.
Farewell to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!
Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?

$4 > 3$? Yes!

$4 > 3 \pmod{7}$? Yes...maybe?

$-3 > 3 \pmod{7}$? Uh oh.. $-3 = 4 \pmod{7}$.

Another problem.

4 is close to 3.
But can you get closer? Sure. 3.5. Closer. Sure? 3.25, 3.1, 3.000001. …

For reals numbers we have the notion of limit, continuity, and derivative…….

....and Calculus.

For modular arithmetic...no Calculus. Sad face!
Next up: how big is infinity.
Next up: how big is infinity.

- Countable
- Countably infinite.
- Enumeration
How big are the reals or the integers?

Infinite!
How big are the reals or the integers?

Infinite!

Is one bigger or smaller?
Same size?

- \( f(\text{red circle}) = \text{red square} \)
- \( f(\text{blue circle}) = \text{blue square} \)
- \( f(\text{circle with black border}) = \text{square with black border} \)

One to one: For all \( x, y \in D \), \( x \neq y \implies f(x) \neq f(y) \).

Onto: For all \( s \in R \), there exists \( c \in D \) such that \( s = f(c) \).

Isomorphism principle: If there is \( f: D \to R \) that is one to one and onto, then, \( |D| = |R| \).
Same size?

Same number?

Make a function $f$: Circles $\rightarrow$ Squares.

$f$(red circle) = red square

$f$(blue circle) = blue square

$f$(circle with black border) = square with black border

One to one. Each circle mapped to different square.

One to One: For all $x, y \in D$, $x \neq y \Rightarrow f(x) \neq f(y)$.

Onto. Each square mapped to from some circle.

Onto: For all $s \in R$, $\exists c \in D, s = f(c)$.

Isomorphism principle: If there is $f: D \rightarrow R$ that is one to one and onto, then, $|D| = |R|$.
Same size?

Same number?
Make a function $f: \text{Circles} \rightarrow \text{Squares}$.
Same size?

Make a function \( f : \text{Circles} \rightarrow \text{Squares} \).

\( f(\text{red circle}) = \text{red square} \)

Same number?

One to one. Each circle mapped to a different square. For all \( x, y \in D \), \( x \neq y \implies f(x) \neq f(y) \).

Onto. Each square mapped from some circle. For all \( s \in R \), there exists \( c \in D \), such that \( s = f(c) \).

Isomorphism principle: If there is \( f : D \rightarrow R \) that is one to one and onto, then, \( |D| = |R| \).
Same size?

Same number?
Make a function $f : \text{Circles} \rightarrow \text{Squares}$.
\[ f(\text{red circle}) = \text{red square} \]
\[ f(\text{blue circle}) = \text{blue square} \]
Same size?

Same number?
Make a function $f : \text{Circles} \to \text{Squares}$.

- $f(\text{red circle}) = \text{red square}$
- $f(\text{blue circle}) = \text{blue square}$
- $f(\text{circle with black border}) = \text{square with black border}$
Same size?

Same number?
Make a function \( f : \text{Circles} \to \text{Squares} \).
\[
\begin{align*}
  f(\text{red circle}) &= \text{red square} \\
  f(\text{blue circle}) &= \text{blue square} \\
  f(\text{circle with black border}) &= \text{square with black border}
\end{align*}
\]
One to one.

Onto.
Each square mapped to from some circle.

Isomorphism principle:
If there is \( f : D \to R \) that is one to one and onto, then,
\[
|D| = |R|.
\]
Same size?

Make a function $f : \text{Circles} \rightarrow \text{Squares}$.

- $f(\text{red circle}) = \text{red square}$
- $f(\text{blue circle}) = \text{blue square}$
- $f(\text{circle with black border}) = \text{square with black border}$

One to one. Each circle mapped to different square.

Same number?
Same size?

Make a function $f : \text{Circles} \rightarrow \text{Squares}$.

- $f(\text{red circle}) = \text{red square}$
- $f(\text{blue circle}) = \text{blue square}$
- $f(\text{circle with black border}) = \text{square with black border}$

One to one. Each circle mapped to different square.

One to One: For all $x, y \in D$, $x \neq y \implies f(x) \neq f(y)$. 

Onto.

Each square mapped to from some circle.

Onto: For all $s \in R$, $\exists c \in D$, $s = f(c)$. 

Isomorphism principle: If there is $f : D \rightarrow R$ that is one to one and onto, then, $|D| = |R|$. 
Same size?

Same number?
Make a function $f : \text{Circles} \rightarrow \text{Squares}$.

$f(\text{red circle}) = \text{red square}$
$f(\text{blue circle}) = \text{blue square}$
$f(\text{circle with black border}) = \text{square with black border}$

One to one. Each circle mapped to different square.

One to One: For all $x, y \in D$, $x \neq y \implies f(x) \neq f(y)$.

Onto.
Same size?

Same number?
Make a function $f : \text{Circles} \rightarrow \text{Squares}$. 
$f(\text{red circle}) = \text{red square}$
$f(\text{blue circle}) = \text{blue square}$
$f(\text{circle with black border}) = \text{square with black border}$

One to one. Each circle mapped to different square.
One to One: For all $x, y \in D$, $x \neq y \implies f(x) \neq f(y)$.

Onto. Each square mapped to from some circle.
Same size?

Make a function $f : \text{Circles} \rightarrow \text{Squares}$.

$\text{f(red circle)} = \text{red square}$

$f(\text{blue circle}) = \text{blue square}$

$f(\text{circle with black border}) = \text{square with black border}$

One to one. Each circle mapped to different square.

One to One: For all $x, y \in D, x \neq y \implies f(x) \neq f(y)$.

Onto. Each square mapped to from some circle.

Onto: For all $s \in R, \exists c \in D, s = f(c)$.
Same size?

Make a function $f : \text{Circles} \to \text{Squares}$.

- $f(\text{red circle}) = \text{red square}$
- $f(\text{blue circle}) = \text{blue square}$
- $f(\text{circle with black border}) = \text{square with black border}$

One to one. Each circle mapped to different square.

One to One: For all $x, y \in D$, $x \neq y \implies f(x) \neq f(y)$.

Onto. Each square mapped to from some circle.

Onto: For all $s \in R$, $\exists c \in D$, $s = f(c)$. 
Same size?

Same number?
Make a function $f : \text{Circles} \rightarrow \text{Squares}$.

$f(\text{red circle}) = \text{red square}$
$f(\text{blue circle}) = \text{blue square}$
$f(\text{circle with black border}) = \text{square with black border}$

One to one. Each circle mapped to different square.

One to One: For all $x, y \in D$, $x \neq y \implies f(x) \neq f(y)$.

Onto. Each square mapped to from some circle.

Onto: For all $s \in R$, $\exists c \in D$, $s = f(c)$.

**Isomorphism principle:** If there is $f : D \rightarrow R$ that is one to one and onto, then, $|D| = |R|$. 
Isomorphism principle.

Given a function, \( f : D \to R \).
Isomorphism principle.

Given a function, \( f : D \rightarrow R \).

**One to One:**
Isomorphism principle.

Given a function, \( f : D \rightarrow R \).

**One to One:**
For all \( \forall x, y \in D, x \neq y \implies f(x) \neq f(y) \).

\[ \text{or} \quad \forall x, y \in D, \quad f(x) = f(y) \implies x = y. \]

**Onto:**
For all \( y \in R \), \( \exists x \in D, y = f(x) \).

\( f(\cdot) \) is a bijection if it is one to one and onto.

Isomorphism principle:
If there is a bijection \( f : D \rightarrow R \) then \( |D| = |R| \).
Given a function, \( f : D \rightarrow R \).

**One to One:**
For all \( \forall x, y \in D, x \neq y \implies f(x) \neq f(y) \).

or

**Onto:**
For all \( \forall y \in R, \exists x \in D, y = f(x) \).

\( f(\cdot) \) is a bijection if it is one to one and onto.

**Isomorphism principle:**
If there is a bijection \( f : D \rightarrow R \) then \( |D| = |R| \).
Isomorphism principle.

Given a function, \( f : D \rightarrow R \).

**One to One:**
For all \( \forall x, y \in D, x \neq y \implies f(x) \neq f(y) \).

or

\( \forall x, y \in D, f(x) = f(y) \implies x = y \).
Isomorphism principle.

Given a function, $f : D \rightarrow R$.

**One to One:**
For all $\forall x, y \in D$, $x \neq y \implies f(x) \neq f(y)$.

or

$\forall x, y \in D$, $f(x) = f(y) \implies x = y$. 
Isomorphism principle.

Given a function, \( f : D \rightarrow R \).

**One to One:**
For all \( \forall x, y \in D, x \neq y \implies f(x) \neq f(y) \).

or

\( \forall x, y \in D, f(x) = f(y) \implies x = y \).

**Onto:** For all \( y \in R, \exists x \in D, y = f(x) \).
Isomorphism principle.

Given a function, $f : D \rightarrow R$.

**One to One:**
For all $\forall x, y \in D$, $x \neq y \implies f(x) \neq f(y)$.

or

$\forall x, y \in D$, $f(x) = f(y) \implies x = y$.

**Onto:** For all $y \in R$, $\exists x \in D$, $y = f(x)$.

$f(\cdot)$ is a **bijection** if it is one to one and onto.
Isomorphism principle.

Given a function, $f : D \to R$.

**One to One:**
For all $\forall x, y \in D$, $x \neq y \implies f(x) \neq f(y)$.

or
$\forall x, y \in D$, $f(x) = f(y) \implies x = y$.

**Onto:** For all $y \in R$, $\exists x \in D$, $y = f(x)$.

$f(\cdot)$ is a **bijection** if it is one to one and onto.

Isomorphism principle:
Isomorphism principle.

Given a function, $f : D \rightarrow R$.

**One to One:**
For all $\forall x, y \in D$, $x \neq y \implies f(x) \neq f(y)$.

or

$\forall x, y \in D$, $f(x) = f(y) \implies x = y$.

**Onto:** For all $y \in R$, $\exists x \in D$, $y = f(x)$.

$f(\cdot)$ is a **bijection** if it is one to one and onto.

**Isomorphism principle:**
If there is a bijection $f : D \rightarrow R$ then $|D| = |R|$.
Countable.

How to count?
Countable.

How to count?

0,
Countable.

How to count?
0, 1,
Countable.

How to count?

0, 1, 2,
Countable.

How to count?
0, 1, 2, 3,
Countable.

How to count?
0, 1, 2, 3, …
Countable.

How to count?
0, 1, 2, 3, …
The Counting numbers.
Countable.

How to count?
0, 1, 2, 3, ...  
The Counting numbers.
The natural numbers! $\mathbb{N}$
How to count?
0, 1, 2, 3, ...

The Counting numbers.
The natural numbers! $N$

Definition: $S$ is **countable** if there is a bijection between $S$ and some subset of $N$. 
Countable.

How to count?

0, 1, 2, 3, …

The Counting numbers.
The natural numbers! $N$

Definition: $S$ is **countable** if there is a bijection between $S$ and some subset of $N$.

If the subset of $N$ is finite, $S$ has finite **cardinality**.
Countable.

How to count?
0, 1, 2, 3, …

The Counting numbers.
The natural numbers! \( N \)

Definition: \( S \) is **countable** if there is a bijection between \( S \) and some subset of \( N \).

If the subset of \( N \) is finite, \( S \) has finite **cardinality**.
If the subset of \( N \) is infinite, \( S \) is **countably infinite**.
Where’s 0?

Which is bigger?

Positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$.

Natural numbers: 0, 1, 2, 3, ...

Positive integers: 1, 2, 3, ...

Where’s 0? More natural numbers!

Consider $f(z) = z - 1$.

For any two $z_1 \neq z_2$, $z_1 - 1 \neq z_2 - 1 \Rightarrow f(z_1) \neq f(z_2)$.

One to one!

For any natural number $n$, for $z = n + 1$, $f(z) = (n + 1) - 1 = n$.

Onto for $\mathbb{N}$!

Bijection! $\Rightarrow |\mathbb{Z}^+| = |\mathbb{N}|$.

But.. but Where’s zero? "Comes from 1."
Where’s 0?

Which is bigger?
The positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$. 
Where’s 0?

Which is bigger? The positive integers, \( \mathbb{Z}^+ \), or the natural numbers, \( \mathbb{N} \).

Natural numbers. 0,
Where’s 0?

Which is bigger?
The positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$.

Natural numbers. 0, 1,
Where’s 0?

Which is bigger?
The positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$.
Natural numbers. 0, 1, 2,
Where’s 0?

Which is bigger?
The positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$.

Natural numbers. 0, 1, 2, 3,
Where’s 0?

Which is bigger?
The positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$.
Natural numbers. 0, 1, 2, 3, ….
Where’s 0?

Which is bigger?
The positive integers, \( \mathbb{Z}^+ \), or the natural numbers, \( \mathbb{N} \).

Natural numbers. 0, 1, 2, 3, ....

Positive integers. 1,
Where’s 0?

Which is bigger?
The positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$.

Natural numbers. 0, 1, 2, 3, ....

Positive integers. 1, 2,
Where’s 0?

Which is bigger?
The positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$.

Natural numbers. 0, 1, 2, 3, ....

Positive integers. 1, 2, 3,
Where’s 0?

Which is bigger?
The positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$.

Natural numbers. 0, 1, 2, 3, ….  
Positive integers. 1, 2, 3, ….
Where’s 0?

Which is bigger?
The positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$.

Natural numbers. 0, 1, 2, 3, ....

Positive integers. 1, 2, 3, ....

Where’s 0?
Where's 0?

Which is bigger?
The positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$.

Natural numbers. 0, 1, 2, 3, ....

Positive integers. 1, 2, 3, ....

Where's 0?

More natural numbers!
Where’s 0?

Which is bigger?
The positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$.

Natural numbers. 0, 1, 2, 3, ... .

Positive integers. 1, 2, 3, ... .

Where’s 0?

More natural numbers!

Consider $f(z) = z - 1$. 
Where’s 0?

Which is bigger?
The positive integers, \( \mathbb{Z}^+ \), or the natural numbers, \( \mathbb{N} \).

Natural numbers. 0, 1, 2, 3, ….

Positive integers. 1, 2, 3, ….

Where’s 0?

More natural numbers!

Consider \( f(z) = z - 1 \).

For any two \( z_1 \neq z_2 \)
Where’s 0?

Which is bigger?
The positive integers, \( \mathbb{Z}^+ \), or the natural numbers, \( \mathbb{N} \).

Natural numbers. 0, 1, 2, 3, ….

Positive integers. 1, 2, 3, ….

Where’s 0?

More natural numbers!

Consider \( f(z) = z - 1 \).

For any two \( z_1 \neq z_2 \) \( \implies \) \( z_1 - 1 \neq z_2 - 1 \).
Where’s 0?

Which is bigger?
The positive integers, \( \mathbb{Z}^+ \), or the natural numbers, \( \mathbb{N} \).
Natural numbers. 0, 1, 2, 3, ….
Positive integers. 1, 2, 3, ….
Where’s 0?
More natural numbers!
Consider \( f(z) = z - 1 \).
For any two \( z_1 \neq z_2 \implies z_1 - 1 \neq z_2 - 1 \implies f(z_1) \neq f(z_2) \).
Where’s 0?

Which is bigger?
The positive integers, \( \mathbb{Z}^+ \), or the natural numbers, \( \mathbb{N} \).

Natural numbers. 0, 1, 2, 3, ....

Positive integers. 1, 2, 3, ....

Where’s 0?

More natural numbers!

Consider \( f(z) = z - 1 \).

For any two \( z_1 \neq z_2 \implies z_1 - 1 \neq z_2 - 1 \implies f(z_1) \neq f(z_2) \).

One to one!
Where’s 0?

Which is bigger?
The positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$.

Natural numbers. 0, 1, 2, 3, ....

Positive integers. 1, 2, 3, ....

Where’s 0?

More natural numbers!

Consider $f(z) = z - 1$.

For any two $z_1 \neq z_2 \implies z_1 - 1 \neq z_2 - 1 \implies f(z_1) \neq f(z_2)$.

One to one!

For any natural number $n$,
Where’s 0?

Which is bigger?
The positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$.

Natural numbers. 0, 1, 2, 3, ....

Positive integers. 1, 2, 3, ....

Where’s 0?

More natural numbers!

Consider $f(z) = z - 1$.

For any two $z_1 \neq z_2 \implies z_1 - 1 \neq z_2 - 1 \implies f(z_1) \neq f(z_2)$.

One to one!

For any natural number $n$, for $z = n + 1$, 

Where’s 0?

Which is bigger?
The positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$.
Natural numbers. 0, 1, 2, 3, ….
Positive integers. 1, 2, 3, ….
Where’s 0?
More natural numbers!
Consider $f(z) = z - 1$.
For any two $z_1 \neq z_2 \implies z_1 - 1 \neq z_2 - 1 \implies f(z_1) \neq f(z_2)$.
One to one!
For any natural number $n$, for $z = n + 1$, $f(z)$
Where’s 0?

Which is bigger? The positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$.

Natural numbers. 0, 1, 2, 3, ....

Positive integers. 1, 2, 3, ....

Where’s 0?

More natural numbers!

Consider $f(z) = z - 1$.

For any two $z_1 \neq z_2 \implies z_1 - 1 \neq z_2 - 1 \implies f(z_1) \neq f(z_2)$. One to one!

For any natural number $n$, for $z = n + 1$, $f(z) = (n + 1) - 1$.
Where’s 0?

Which is bigger?
The positive integers, \( \mathbb{Z}^+ \), or the natural numbers, \( \mathbb{N} \).

Natural numbers. 0, 1, 2, 3, ....

Positive integers. 1, 2, 3, ....

Where’s 0?

More natural numbers!

Consider \( f(z) = z - 1 \).

For any two \( z_1 \neq z_2 \implies z_1 - 1 \neq z_2 - 1 \implies f(z_1) \neq f(z_2) \).

One to one!

For any natural number \( n \), for \( z = n + 1 \), \( f(z) = (n + 1) - 1 = n \).
Where’s 0?

Which is bigger?
The positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$.

Natural numbers. 0, 1, 2, 3, ....

Positive integers. 1, 2, 3, ....

Where’s 0?

More natural numbers!

Consider $f(z) = z - 1$.

For any two $z_1 \neq z_2 \implies z_1 - 1 \neq z_2 - 1 \implies f(z_1) \neq f(z_2)$.

One to one!

For any natural number $n$, for $z = n + 1$, $f(z) = (n + 1) - 1 = n$.

Onto for $\mathbb{N}$
Where’s 0?

Which is bigger?
The positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$.

Natural numbers. 0, 1, 2, 3, ....

Positive integers. 1, 2, 3, ....

Where’s 0?

More natural numbers!

Consider $f(z) = z - 1$.

For any two $z_1 \neq z_2 \implies z_1 - 1 \neq z_2 - 1 \implies f(z_1) \neq f(z_2)$.

One to one!

For any natural number $n$, for $z = n + 1$ , $f(z) = (n + 1) - 1 = n$.

Onto for $\mathbb{N}$

Bijection!
Where’s 0?

Which is bigger?
The positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$.

Natural numbers. 0, 1, 2, 3, ....

Positive integers. 1, 2, 3, ....

Where’s 0?

More natural numbers!

Consider $f(z) = z - 1$.

For any two $z_1 \neq z_2 \implies z_1 - 1 \neq z_2 - 1 \implies f(z_1) \neq f(z_2)$. One to one!

For any natural number $n$, for $z = n + 1$, $f(z) = (n + 1) - 1 = n$. Onto for $\mathbb{N}$

Bijection! $\implies |\mathbb{Z}^+| = |\mathbb{N}|$. 
Where’s 0?

Which is bigger?
The positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$.

Natural numbers. 0, 1, 2, 3, ....

Positive integers. 1, 2, 3, ....

Where’s 0?

More natural numbers!

Consider $f(z) = z - 1$.

For any two $z_1 \neq z_2 \implies z_1 - 1 \neq z_2 - 1 \implies f(z_1) \neq f(z_2)$.

One to one!

For any natural number $n$, for $z = n + 1$, $f(z) = (n + 1) - 1 = n$.

Onto for $\mathbb{N}$

Bijection! $\implies |\mathbb{Z}^+| = |\mathbb{N}|$.

But.. but
Where's 0?

Which is bigger?
The positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$.

Natural numbers. 0, 1, 2, 3, ....

Positive integers. 1, 2, 3, ....

Where's 0?

More natural numbers!

Consider $f(z) = z - 1$.

For any two $z_1 \neq z_2 \implies z_1 - 1 \neq z_2 - 1 \implies f(z_1) \neq f(z_2)$.

One to one!

For any natural number $n$, for $z = n + 1$, $f(z) = (n + 1) - 1 = n$.

Onto for $\mathbb{N}$

Bijection! $\implies |\mathbb{Z}^+| = |\mathbb{N}|$.

But.. but Where's zero?
Where’s 0?

Which is bigger?
The positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$.

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1, 2, 3, \ldots$.

Where’s 0?

More natural numbers!

Consider $f(z) = z - 1$.

For any two $z_1 \neq z_2 \implies z_1 - 1 \neq z_2 - 1 \implies f(z_1) \neq f(z_2)$.

One to one!

For any natural number $n$, for $z = n + 1$, $f(z) = (n + 1) - 1 = n$.

Onto for $\mathbb{N}$

Bijection! $\implies |\mathbb{Z}^+| = |\mathbb{N}|$.

But.. but Where’s zero? “Comes from 1.”
A bijection is a bijection.
A bijection is a bijection.

Notice that there is a bijection between $N$ and $Z^+$ as well.
A bijection is a bijection.

Notice that there is a bijection between $N$ and $Z^+$ as well.  
$f(n) = n + 1$. 
A bijection is a bijection.

Notice that there is a bijection between \( N \) and \( Z^+ \) as well. \( f(n) = n + 1 \). 0 \( \rightarrow \) 1,
A bijection is a bijection.

Notice that there is a bijection between \( N \) and \( Z^+ \) as well. 
\[ f(n) = n + 1. \ 0 \rightarrow 1, \ 1 \rightarrow 2, \]
A bijection is a bijection.

Notice that there is a bijection between $N$ and $Z^+$ as well. $f(n) = n + 1$. $0 \rightarrow 1, 1 \rightarrow 2, \ldots$
A bijection is a bijection.

Notice that there is a bijection between \( N \) and \( \mathbb{Z}^+ \) as well.

\[ f(n) = n + 1. \quad 0 \rightarrow 1, \ 1 \rightarrow 2, \ldots \]

Bijection from \( A \) to \( B \) \( \implies \) a bijection from \( B \) to \( A \).
A bijection is a bijection.

Notice that there is a bijection between $N$ and $Z^+$ as well. 
$f(n) = n + 1$. $0 \rightarrow 1, 1 \rightarrow 2, \ldots$

Bijection from $A$ to $B \implies$ a bijection from $B$ to $A$. 
A bijection is a bijection.

Notice that there is a bijection between $N$ and $Z^+$ as well. $f(n) = n + 1$. $0 \rightarrow 1, 1 \rightarrow 2, \ldots$

Bijection from $A$ to $B \implies$ a bijection from $B$ to $A$.

Inverse function!
A bijection is a bijection.

Notice that there is a bijection between $N$ and $\mathbb{Z}^+$ as well. $f(n) = n + 1$. $0 \rightarrow 1, 1 \rightarrow 2, \ldots$

Bijection from $A$ to $B \implies$ a bijection from $B$ to $A$.

Inverse function!

Can prove equivalence either way.
A bijection is a bijection.

Notice that there is a bijection between $\mathbb{N}$ and $\mathbb{Z}^+$ as well.

\[ f(n) = n + 1. \quad 0 \rightarrow 1, 1 \rightarrow 2, \ldots \]

Bijection from $A$ to $B$ $\implies$ a bijection from $B$ to $A$.

Inverse function!

Can prove equivalence either way.
Bijection to or from natural numbers implies countably infinite.
More large sets.

\[ E - \text{Even natural numbers?} \]
More large sets.

$E$ - Even natural numbers?

$f : N \to E.$

Evens are countably infinite.
Evens are same size as all natural numbers.
$E$ - Even natural numbers?

$f : N \to E.$

$f(n) \to 2n.$
More large sets.

\[ E - \text{Even natural numbers?} \]

\[ f : N \rightarrow E. \]

\[ f(n) \rightarrow 2n. \]

Onto:
More large sets.

\( E \) - Even natural numbers?  
\( f: N \to E. \)  
\( f(n) \to 2n. \)  
Onto: \( \forall e \in E, f(e/2) = e. \)
More large sets.

$E$ - Even natural numbers?

$f : N \rightarrow E.$

$f(n) \rightarrow 2n.$

Onto: $\forall e \in E, f(e/2) = e.$ $e/2$ is natural since $e$ is even
More large sets.

$E$ - Even natural numbers?

$f : N \to E.$

$f(n) \to 2n.$

Onto: $\forall e \in E, f(e/2) = e.$ $e/2$ is natural since $e$ is even

One-to-one:
More large sets.

$E$ - Even natural numbers?

$f : N \rightarrow E.$

$f(n) \rightarrow 2n.$

Onto: $\forall e \in E, f(e/2) = e.$ $e/2$ is natural since $e$ is even

One-to-one: $\forall x, y \in N, x \neq y \implies 2x \neq 2y.$
More large sets.

$E$ - Even natural numbers?

$f : N \rightarrow E.$

$f(n) \rightarrow 2n.$

Onto: $\forall e \in E, \ f(e/2) = e.$ $e/2$ is natural since $e$ is even

One-to-one: $\forall x, y \in N, x \neq y \implies 2x \neq 2y. \equiv f(x) \neq f(y)$
More large sets.

$E$ - Even natural numbers?

$f : N \rightarrow E.$

$f(n) \rightarrow 2n.$

Onto: $\forall e \in E, \, f(e/2) = e.$ $e/2$ is natural since $e$ is even

One-to-one: $\forall x, y \in N, \, x \neq y \implies 2x \neq 2y. \equiv f(x) \neq f(y)$

Evens are countably infinite.
More large sets.

\(E\) - Even natural numbers?

\(f : N \rightarrow E.\)

\(f(n) \rightarrow 2n.\)

Onto: \(\forall e \in E, f(e/2) = e.\) \(e/2\) is natural since \(e\) is even

One-to-one: \(\forall x, y \in N, x \neq y \implies 2x \neq 2y.\) \(\equiv f(x) \neq f(y)\)

Evens are countably infinite.
Evens are same size as all natural numbers.
All integers?

What about Integers, $\mathbb{Z}$?
All integers?

What about Integers, \(\mathbb{Z}\)?
Define \(f : \mathbb{N} \to \mathbb{Z}\).

\[
f(n) = \begin{cases} 
  n/2 & \text{if } n \text{ even} \\
  -(n+1)/2 & \text{if } n \text{ odd.}
\end{cases}
\]
All integers?

What about Integers, $\mathbb{Z}$?
Define $f : \mathbb{N} \to \mathbb{Z}$.

$$f(n) = \begin{cases} 
\frac{n}{2} & \text{if } n \text{ even} \\
-(n+1)/2 & \text{if } n \text{ odd}.
\end{cases}$$

One-to-one: For $x \neq y$
All integers?

What about Integers, $\mathbb{Z}$?
Define $f : \mathbb{N} \rightarrow \mathbb{Z}$.

$$f(n) = \begin{cases} 
\frac{n}{2} & \text{if } n \text{ even} \\
-(n+1)/2 & \text{if } n \text{ odd}.
\end{cases}$$

One-to-one: For $x \neq y$
if $x$ is even and $y$ is odd,
All integers?

What about Integers, \( Z \)?
Define \( f : N \rightarrow Z \).

\[
f(n) = \begin{cases} 
  n/2 & \text{if } n \text{ even} \\
  -(n+1)/2 & \text{if } n \text{ odd.}
\end{cases}
\]

One-to-one: For \( x \neq y \)
if \( x \) is even and \( y \) is odd,
then \( f(x) \) is nonnegative and \( f(y) \) is negative

Integers and naturals have same size!
All integers?

What about Integers, $Z$?
Define $f : N \rightarrow Z$.

$$f(n) = \begin{cases} n/2 & \text{if } n \text{ even} \\ -(n+1)/2 & \text{if } n \text{ odd.} \end{cases}$$

One-to-one: For $x \neq y$
if $x$ is even and $y$ is odd,
then $f(x)$ is nonnegative and $f(y)$ is negative  $\implies f(x) \neq f(y)$
All integers?

What about Integers, $\mathbb{Z}$?
Define $f : N \rightarrow \mathbb{Z}$.

$$f(n) = \begin{cases} 
  n/2 & \text{if } n \text{ even} \\
  -(n+1)/2 & \text{if } n \text{ odd.}
\end{cases}$$

One-to-one: For $x \neq y$
if $x$ is even and $y$ is odd,
then $f(x)$ is nonnegative and $f(y)$ is negative $\implies f(x) \neq f(y)$
if $x$ is even and $y$ is even,
All integers?

What about Integers, $\mathbb{Z}$?

Define $f : \mathbb{N} \to \mathbb{Z}$.

$$f(n) = \begin{cases} 
\frac{n}{2} & \text{if } n \text{ even} \\
-(n+1)/2 & \text{if } n \text{ odd.}
\end{cases}$$

One-to-one: For $x \neq y$

if $x$ is even and $y$ is odd,
then $f(x)$ is nonnegative and $f(y)$ is negative $\implies f(x) \neq f(y)$

if $x$ is even and $y$ is even,
then $x/2 \neq y/2$
All integers?

What about Integers, $\mathbb{Z}$?
Define $f : \mathbb{N} \rightarrow \mathbb{Z}$.

$$f(n) = \begin{cases} n/2 & \text{if } n \text{ even} \\ -(n + 1)/2 & \text{if } n \text{ odd} \end{cases}$$

One-to-one: For $x \neq y$
if $x$ is even and $y$ is odd,
then $f(x)$ is nonnegative and $f(y)$ is negative $\implies f(x) \neq f(y)$
if $x$ is even and $y$ is even,
then $x/2 \neq y/2 \implies f(x) \neq f(y)$
All integers?

What about Integers, $\mathbb{Z}$?
Define $f : N \to \mathbb{Z}$.

$$f(n) = \begin{cases} 
\frac{n}{2} & \text{if } n \text{ even} \\
-(\frac{n+1}{2}) & \text{if } n \text{ odd.}
\end{cases}$$

One-to-one: For $x \neq y$
if $x$ is even and $y$ is odd,
then $f(x)$ is nonnegative and $f(y)$ is negative $\implies f(x) \neq f(y)$
if $x$ is even and $y$ is even,
then $x/2 \neq y/2 \implies f(x) \neq f(y)$

....
All integers?

What about Integers, $Z$?
Define $f : N \rightarrow Z$.

$$f(n) = \begin{cases} 
    n/2 & \text{if } n \text{ even} \\
    -(n+1)/2 & \text{if } n \text{ odd}
\end{cases}$$

One-to-one: For $x \neq y$
if $x$ is even and $y$ is odd,
then $f(x)$ is nonnegative and $f(y)$ is negative $\implies f(x) \neq f(y)$
if $x$ is even and $y$ is even,
then $x/2 \neq y/2 \implies f(x) \neq f(y)$
....

Onto: For any $z \in Z$, 

All integers?

What about Integers, $\mathbb{Z}$?
Define $f : N \rightarrow \mathbb{Z}$.

$$f(n) = \begin{cases} n/2 & \text{if } n \text{ even} \\ -(n+1)/2 & \text{if } n \text{ odd.} \end{cases}$$

One-to-one: For $x \neq y$
if $x$ is even and $y$ is odd,
then $f(x)$ is nonnegative and $f(y)$ is negative $\implies f(x) \neq f(y)$
if $x$ is even and $y$ is even,
then $x/2 \neq y/2 \implies f(x) \neq f(y)$

....

Onto: For any $z \in \mathbb{Z}$,
if $z \geq 0$, $f(2z) = z$ and $2z \in N$. 
All integers?

What about Integers, \( \mathbb{Z} \)?
Define \( f : \mathbb{N} \rightarrow \mathbb{Z} \).

\[
  f(n) = \begin{cases} 
    n/2 & \text{if } n \text{ even} \\
    -(n+1)/2 & \text{if } n \text{ odd}.
  \end{cases}
\]

One-to-one: For \( x \neq y \)
if \( x \) is even and \( y \) is odd,
then \( f(x) \) is nonnegative and \( f(y) \) is negative \( \implies f(x) \neq f(y) \)
if \( x \) is even and \( y \) is even,
then \( x/2 \neq y/2 \implies f(x) \neq f(y) \)
	....

Onto: For any \( z \in \mathbb{Z} \),
if \( z \geq 0 \), \( f(2z) = z \) and \( 2z \in \mathbb{N} \).
if \( z < 0 \), \( f(2|z| - 1) = z \) and \( 2|z| + 1 \in \mathbb{N} \).

Integers and naturals have same size!
All integers?

What about Integers, \( Z \)?
Define \( f : N \rightarrow Z \).

\[
f(n) = \begin{cases} 
  n/2 & \text{if } n \text{ even} \\
  -(n+1)/2 & \text{if } n \text{ odd}.
\end{cases}
\]

One-to-one: For \( x \neq y \)
if \( x \) is even and \( y \) is odd,
then \( f(x) \) is nonnegative and \( f(y) \) is negative \( \implies f(x) \neq f(y) \)
if \( x \) is even and \( y \) is even,
then \( x/2 \neq y/2 \implies f(x) \neq f(y) \)

.....

Onto: For any \( z \in Z \),
if \( z \geq 0 \), \( f(2z) = z \) and \( 2z \in N \).
if \( z < 0 \), \( f(2|z| - 1) = z \) and \( 2|z| + 1 \in N \).

Integers and naturals have same size!
Listings..

\[ f(n) = \begin{cases} 
  n/2 & \text{if } n \text{ even} \\
  -(n+1)/2 & \text{if } n \text{ odd.} 
\end{cases} \]

Another View:

\[
\begin{array}{cccc}
0 & 0 & 1 & -1 \\
2 & 1 & 3 & -2 \\
& ... & ... & ...
\end{array}
\]

Notice that: A listing “is” a bijection with a subset of natural numbers.

Function \equiv “Position in list.”

If finite: bijection with \{0,...,|S|−1\}

If infinite: bijection with \mathbb{N}. 
Listings..

\[ f(n) = \begin{cases} 
  n/2 & \text{if } n \text{ even} \\
  -(n+1)/2 & \text{if } n \text{ odd.} 
\end{cases} \]

Another View:

<table>
<thead>
<tr>
<th>( n )</th>
<th>( f(n) )</th>
</tr>
</thead>
</table>

Notice that: A listing “is” a bijection with a subset of natural numbers. Function \( \equiv \) “Position in list.” If finite: bijection with \( \{0, \ldots, |S| - 1\} \). If infinite: bijection with \( \mathbb{N} \).
Listings...

\[ f(n) = \begin{cases} 
  n/2 & \text{if } n \text{ even} \\
  -(n+1)/2 & \text{if } n \text{ odd.}
\end{cases} \]

Another View:

<table>
<thead>
<tr>
<th>( n )</th>
<th>( f(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Listings..

\[ f(n) = \begin{cases} 
  n/2 & \text{if } n \text{ even} \\
  -(n+1)/2 & \text{if } n \text{ odd.}
\end{cases} \]

Another View:

<table>
<thead>
<tr>
<th>( n )</th>
<th>( f(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>−1</td>
</tr>
</tbody>
</table>
Listings..

$$f(n) = \begin{cases} 
\frac{n}{2} & \text{if } n \text{ even} \\
-\frac{n+1}{2} & \text{if } n \text{ odd.}
\end{cases}$$

Another View:

<table>
<thead>
<tr>
<th>$n$</th>
<th>$f(n)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
Listings..

\[ f(n) = \begin{cases} 
  n/2 & \text{if } n \text{ even} \\
  -(n+1)/2 & \text{if } n \text{ odd.}
\end{cases} \]

Another View:

<table>
<thead>
<tr>
<th>( n )</th>
<th>( f(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>-2</td>
</tr>
</tbody>
</table>
Listings..

\[ f(n) = \begin{cases} 
  n/2 & \text{if } n \text{ even} \\
  -(n+1)/2 & \text{if } n \text{ odd.} 
\end{cases} \]

Another View:

<table>
<thead>
<tr>
<th>( n )</th>
<th>( f(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>-2</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
</tr>
</tbody>
</table>
Listings..

\[ f(n) = \begin{cases} 
  \frac{n}{2} & \text{if } n \text{ even} \\
  -\frac{n+1}{2} & \text{if } n \text{ odd.} 
\end{cases} \]

Another View:

<table>
<thead>
<tr>
<th>( n )</th>
<th>( f(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>-2</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
Listings..

\[ f(n) = \begin{cases} 
  n/2 & \text{if } n \text{ even} \\
  -(n+1)/2 & \text{if } n \text{ odd.} 
\end{cases} \]

Another View:

<table>
<thead>
<tr>
<th>( n )</th>
<th>( f(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>-2</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>( \ldots )</td>
<td>( \ldots )</td>
</tr>
</tbody>
</table>

Notice that: A listing “is” a bijection with a subset of natural numbers.
Listings...

\[ f(n) = \begin{cases} 
    n/2 & \text{if } n \text{ even} \\
    -(n+1)/2 & \text{if } n \text{ odd.}
\end{cases} \]

Another View:

<table>
<thead>
<tr>
<th>( n )</th>
<th>( f(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>-2</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>\ldots</td>
<td>\ldots</td>
</tr>
</tbody>
</table>

Notice that: A listing “is” a bijection with a subset of natural numbers. Function \( \equiv \) “Position in list.”
Listings...

\[ f(n) = \begin{cases} 
  n/2 & \text{if } n \text{ even} \\
  -(n+1)/2 & \text{if } n \text{ odd.} 
\end{cases} \]

Another View:

<table>
<thead>
<tr>
<th>( n )</th>
<th>( f(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>-2</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Notice that: A listing “is” a bijection with a subset of natural numbers. Function ≡ “Position in list.”
If finite: bijection with \( \{0, \ldots, |S| - 1\} \)
Listings..

\[ f(n) = \begin{cases} 
  n/2 & \text{if } n \text{ even} \\
  -(n+1)/2 & \text{if } n \text{ odd.}
\end{cases} \]

Another View:

<table>
<thead>
<tr>
<th>( n )</th>
<th>( f(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>-2</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Notice that: A listing “is” a bijection with a subset of natural numbers.
Function \( \equiv \) “Position in list.”
If finite: bijection with \( \{0, \ldots, |S| - 1\} \)
If infinite: bijection with \( \mathbb{N} \).
Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.
Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.
Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

“Output element of $S$”,

$Z = \{0, 1, -1, 2, -2, \ldots\}$

When do you get to $-1$ at infinity?

Need to be careful.
Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

“Output element of $S$”,
“Output next element of $S$”
Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

“Output element of $S$”,
“Output next element of $S$”

...
Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

“Output element of $S$”,
“Output next element of $S$”

... Any element $x$ of $S$ has specific, finite position in list.
Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

“Output element of $S$”,
“Output next element of $S$”

... Any element $x$ of $S$ has specific, finite position in list.

$Z = \{0,$
Enumerability \equiv \text{countability.}

Enumerating (listing) a set implies that it is countable.

“Output element of $S$”,
“Output next element of $S$”

\ldots

Any element $x$ of $S$ has \textit{specific, finite} position in list.

$Z = \{0, 1,$
Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

“Output element of $S$”,
“Output next element of $S$”

$\ldots$

Any element $x$ of $S$ has specific, finite position in list.

$Z = \{0, 1, -1, \ldots\}$
Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

“Output element of $S$”,
“Output next element of $S$”

…

Any element $x$ of $S$ has specific, finite position in list.

$Z = \{0, 1, -1, 2, \ldots\}$
Enumerability ≡ countability.

Enumerating (listing) a set implies that it is countable.

“Output element of $S$”,
“Output next element of $S$”

…

Any element $x$ of $S$ has specific, finite position in list.

$Z = \{0, 1, -1, 2, -2,$
Enumerability \equiv countability.

Enumerating (listing) a set implies that it is countable.

“Output element of $S$”,
“Output next element of $S$”

... Any element $x$ of $S$ has specific, finite position in list.

$Z = \{0, 1, -1, 2, -2, \ldots\}$
Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

“Output element of $S$”,
“Output next element of $S$”

... Any element $x$ of $S$ has specific, finite position in list.
$Z = \{0, 1, -1, 2, -2, \ldots\}$
$Z = \{0, 1, 2, \ldots, \}$

---

When do you get to $-1$ at infinity? Need to be careful.
Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

"Output element of $S$",
"Output next element of $S$"

... Any element $x$ of $S$ has specific, finite position in list.

$Z = \{0, 1, -1, 2, -2, \ldots\}$

$Z = \{\{0, 1, 2, \ldots\}\}$ and then $\{-1, -2, \ldots\}$
Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

“Output element of $S$”,
“Output next element of $S$”

... Any element $x$ of $S$ has specific, finite position in list.
$Z = \{0, 1, -1, 2, -2, \ldots\}$
$Z = \{\{0, 1, 2, \ldots, \} \text{ and then } \{-1, -2, \ldots\}\}$

When do you get to $-1$?
Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

“Output element of $S$”,
“Output next element of $S$”

... Any element $x$ of $S$ has specific, finite position in list.
$Z = \{0, 1, -1, 2, -2, \ldots\}$
$Z = \{0, 1, 2, \ldots, \}$ and then $\{-1, -2, \ldots\}$

When do you get to $-1$? at infinity?
Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

“Output element of $S$”,
“Output next element of $S$”

…

Any element $x$ of $S$ has specific, finite position in list.

$Z = \{0, 1, -1, 2, -2, \ldots\}$

$Z = \{\{0, 1, 2, \ldots,\} \text{ and then } \{-1, -2, \ldots\}\}$

When do you get to $-1$? at infinity?

Need to be careful.
Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

“Output element of $S$”,
“Output next element of $S$”

... Any element $x$ of $S$ has *specific, finite* position in list.

$Z = \{0, 1, -1, 2, -2, \ldots\}$

$Z = \{\{0, 1, 2, \ldots\}\}$ and then $\{-1, -2, \ldots\}$

When do you get to $-1$? at infinity? 

Need to be careful.

61A
Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

“Output element of $S$”,
“Output next element of $S$”

…

Any element $x$ of $S$ has *specific, finite* position in list.

$Z = \{0, 1, -1, 2, -2, \ldots\}$

$Z = \{\{0, 1, 2, \ldots\}\}$ and then $\{-1, -2, \ldots\}$

When do you get to $-1$? at infinity?

Need to be careful.

61A —- streams!
Countably infinite subsets.

Enumerating a set implies countable.
Corollary: Any subset $T$ of a countable set $S$ is countable.
Enumerating a set implies countable.
Corollary: Any subset $T$ of a countable set $S$ is countable.
Enumerate $T$ as follows:
Countably infinite subsets.

Enumerating a set implies countable.
Corollary: Any subset \( T \) of a countable set \( S \) is countable.

Enumerate \( T \) as follows:
Get next element, \( x \), of \( S \),
Countably infinite subsets.

Enumerating a set implies countable.
Corollary: Any subset $T$ of a countable set $S$ is countable.

Enumerate $T$ as follows:
Get next element, $x$, of $S$,
output only if $x \in T$. 
Countably infinite subsets.

Enumerating a set implies countable.
Corollary: Any subset $T$ of a countable set $S$ is countable.

Enumerate $T$ as follows:
Get next element, $x$, of $S$,
output only if $x \in T$. 

Implications:
$\mathbb{Z}^+$ is countable.
It is infinite since the list goes on.
There is a bijection with the natural numbers.
So it is countably infinite.
All countably infinite sets have the same cardinality.
Countably infinite subsets.

Enumerating a set implies countable.  
Corollary: Any subset $T$ of a countable set $S$ is countable.  

Enumerate $T$ as follows:  
Get next element, $x$, of $S$,  
output only if $x \in T$.  

Implications:
Enumerating a set implies countable. Corollary: Any subset $T$ of a countable set $S$ is countable.

Enumerate $T$ as follows:
Get next element, $x$, of $S$, output only if $x \in T$.

Implications:
$\mathbb{Z}^+$ is countable.
Enumerating a set implies countable. 
Corollary: Any subset $T$ of a countable set $S$ is countable.

Enumerate $T$ as follows:
Get next element, $x$, of $S$,
output only if $x \in T$.

Implications:
$\mathbb{Z}^+$ is countable.
It is infinite since the list goes on.
Enumerating a set implies countable. 
Corollary: Any subset $T$ of a countable set $S$ is countable.

Enumerate $T$ as follows: 
Get next element, $x$, of $S$, 
output only if $x \in T$.

Implications: 
$\mathbb{Z}^+$ is countable. 
It is infinite since the list goes on. 
There is a bijection with the natural numbers.
Countably infinite subsets.

Enumerating a set implies countable.  
Corollary: Any subset $T$ of a countable set $S$ is countable.

Enumerate $T$ as follows:
Get next element, $x$, of $S$,
output only if $x \in T$.

Implications:
$\mathbb{Z}^+$ is countable.
It is infinite since the list goes on.
There is a bijection with the natural numbers.
So it is countably infinite.
Countably infinite subsets.

Enumerating a set implies countable.
Corollary: Any subset $T$ of a countable set $S$ is countable.

Enumerate $T$ as follows:
Get next element, $x$, of $S$,
output only if $x \in T$.

Implications:
$\mathbb{Z}^+$ is countable.
It is infinite since the list goes on.
There is a bijection with the natural numbers.
So it is countably infinite.

All countably infinite sets have the same cardinality.
Enumeration example.

All binary strings.
All binary strings.
$B = \{0, 1\}^*$. 
All binary strings.

$B = \{0, 1\}^*$. 

$B = \{\phi, \}$
All binary strings.
\[ B = \{0, 1\}^*. \]
\[ B = \{\phi, 0, \ldots\}. \]
All binary strings.

\[ B = \{0, 1\}^* \]

\[ B = \{\phi, 0, 1, \ldots\} \]

\( \phi \) is empty string.

For any string, it appears at some position in the list.

If \( n \) bits, it will appear before position \( 2^n + 1 \).

Should be careful here.
Enumeration example.

All binary strings.

\[ B = \{0, 1\}^* \]

\[ B = \{\phi, 0, 1, 00, \ldots\} \]

\( \phi \) is empty string.

For any string, it appears at some position in the list. If \( n \) bits, it will appear before position \( 2^n + 1 \).

Should be careful here.
Enumeration example.

All binary strings.

\[ B = \{0, 1\}^* . \]

\[ B = \{ \emptyset, 0, 1, 00, 01, 10, 11, \ldots \} . \]

\( \emptyset \) is empty string.
For any string, it appears at some position in the list.
If \( n \) bits, it will appear before position \( 2^n + 1 \).
Should be careful here.
Enumeration example.

All binary strings. 

\[ B = \{0, 1\}^* \]

\[ B = \{\phi, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, \ldots \} \]
All binary strings.

$B = \{0, 1\}^*.$

$B = \{\phi, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, \ldots\}.$

$\phi$ is empty string.
All binary strings. 
\( B = \{0, 1\}^* \).

\( B = \{\phi, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, \ldots \} \).
\( \phi \) is empty string.

For any string, it appears at some position in the list.
All binary strings.
\( B = \{0, 1\}^* \).

\[ B = \{\phi, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, \ldots\} \]

\( \phi \) is empty string.

For any string, it appears at some position in the list. If \( n \) bits, it will appear before position \( 2^{n+1} \).
All binary strings.

$B = \{0, 1\}^*$. 

$B = \{\phi, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, \ldots\}$. 

$\phi$ is empty string.

For any string, it appears at some position in the list. 
If $n$ bits, it will appear before position $2^{n+1}$.

Should be careful here.
All binary strings. 
\( B = \{0, 1\}^* \).

\( B = \{\phi, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, \ldots\} \).

\( \phi \) is empty string.

For any string, it appears at some position in the list. If \( n \) bits, it will appear before position \( 2^{n+1} \).

Should be careful here.

\( B = \{\phi; 0, 00, 000, 0000, \ldots\} \)
All binary strings.
$B = \{0, 1\}^*$. 

$B = \{\phi, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, \ldots\}$. 
$\phi$ is empty string.

For any string, it appears at some position in the list. 
If $n$ bits, it will appear before position $2^{n+1}$.

Should be careful here.

$B = \{\phi; , 0, 00, 000, 0000, \ldots\}$

Never get to 1.
More fractions?

Enumerate the rational numbers in order...
More fractions?

Enumerate the rational numbers in order...
0, ..., 1/2, ..
More fractions?

Enumerate the rational numbers in order...
0, ..., 1/2, ..
Where is 1/2 in list?
Enumerate the rational numbers in order...
0, ..., 1/2, ..
Where is 1/2 in list?
After 1/3, which is after 1/4, which is after 1/5...
More fractions?

Enumerate the rational numbers in order...

0, ..., 1/2, ...

Where is 1/2 in list?

After 1/3, which is after 1/4, which is after 1/5...

A thing about fractions:
Enumerate the rational numbers in order...
0, ..., 1/2, ...
Where is 1/2 in list?
After 1/3, which is after 1/4, which is after 1/5...
A thing about fractions:
any two fractions has another fraction between it.
Enumerate the rational numbers in order...
0, ..., 1/2, ...

Where is 1/2 in list?

After 1/3, which is after 1/4, which is after 1/5...

A thing about fractions:
any two fractions has another fraction between it.
Can’t even get to “next” fraction!
More fractions?

Enumerate the rational numbers in order...
0, ..., 1/2, ..

Where is 1/2 in list?
After 1/3, which is after 1/4, which is after 1/5...

A thing about fractions:
any two fractions has another fraction between it.
Can’t even get to “next” fraction!
Can’t list in “order”.

Pairs of natural numbers.

Consider pairs of natural numbers: \( N \times N \)
Pairs of natural numbers.

Consider pairs of natural numbers: $\mathbb{N} \times \mathbb{N}$

E.g.: (1, 2), (100, 30), etc.
Pairs of natural numbers.

Consider pairs of natural numbers: $N \times N$
E.g.: (1, 2), (100, 30), etc.
For finite sets $S_1$ and $S_2$, 
Pairs of natural numbers.

Consider pairs of natural numbers: $N \times N$
E.g.: $(1, 2)$, $(100, 30)$, etc.

For finite sets $S_1$ and $S_2$, then $S_1 \times S_2$
Consider pairs of natural numbers: $N \times N$

E.g.: $(1, 2)$, $(100, 30)$, etc.

For finite sets $S_1$ and $S_2$, then $S_1 \times S_2$
has size $|S_1| \times |S_2|$.
Consider pairs of natural numbers: $N \times N$
E.g.: $(1, 2), (100, 30)$, etc.

For finite sets $S_1$ and $S_2$,
then $S_1 \times S_2$
has size $|S_1| \times |S_2|$. 
Consider pairs of natural numbers: \( N \times N \)
E.g.: \((1,2), (100,30)\), etc.

For finite sets \( S_1 \) and \( S_2 \),
then \( S_1 \times S_2 \)
has size \(|S_1| \times |S_2|\).

So, \( N \times N \) is countably infinite
Pairs of natural numbers.

Consider pairs of natural numbers: $N \times N$
E.g.: $(1, 2)$, $(100, 30)$, etc.

For finite sets $S_1$ and $S_2$,
then $S_1 \times S_2$
has size $|S_1| \times |S_2|$.

So, $N \times N$ is countably infinite squared.
Pairs of natural numbers.

Consider pairs of natural numbers: $N \times N$
E.g.: $(1, 2), (100, 30)$, etc.

For finite sets $S_1$ and $S_2$,
then $S_1 \times S_2$
has size $|S_1| \times |S_2|$. 

So, $N \times N$ is countably infinite squared ???
Pairs of natural numbers.

Enumerate in list:

$(0,0)$, $(1,0)$, $(0,1)$, $(2,0)$, $(1,1)$, $(0,2)$,......

The pair $(a,b)$, is in first $(a+b+1)(a+b)/2$ elements of list! (i.e., "triangle").

Countably infinite.

Same size as the natural numbers!!
Pairs of natural numbers.

Enumerate in list:
(0,0),
(1,0),
(0,1),
(2,0),
(1,1),
(0,2),
......
Pairs of natural numbers.

Enumerate in list:
(0,0), (1,0),
Pairs of natural numbers.

Enumerate in list:
(0, 0), (1, 0), (0, 1),
Pairs of natural numbers.

Enumerate in list:
(0,0), (1,0), (0,1), (2,0),...
Pairs of natural numbers.

Enumerate in list:
(0,0), (1,0), (0,1), (2,0), (1,1),
Pairs of natural numbers.

Enumerate in list:

\[(0,0), (1,0), (0,1), (2,0), (1,1), (0,2), \ldots \]

The pair \((a, b)\), is in first \((a + b + 1)(a + b) / 2\) elements of list!

(i.e., “triangle”).

Countably infinite.

Same size as the natural numbers!!
Pairs of natural numbers.

Enumerate in list:
(0, 0), (1, 0), (0, 1), (2, 0), (1, 1), (0, 2), ……
Pairs of natural numbers.

Enumerate in list:

\[(0, 0), (1, 0), (0, 1), (2, 0), (1, 1), (0, 2), \ldots \]

The pair \((a, b)\), is in first \((a + b + 1)(a + b) / 2\) elements of list!

(i.e., "triangle").

Countably infinite.

Same size as the natural numbers!!
Pairs of natural numbers.

Enumerate in list:
(0, 0), (1, 0), (0, 1), (2, 0), (1, 1), (0, 2), ……

The pair \((a, b)\), is in first \((a + b + 1)(a + b) / 2\) elements of list!

(i.e., “triangle”).

Countably infinite.

Same size as the natural numbers!!
Pairs of natural numbers.

Enumerate in list:

\((0,0), (1,0), (0,1), (2,0), (1,1), (0,2), \ldots \)

The pair \((a, b)\), is in first \((a+b+1)(a+b)\) elements of list!

(i.e., “triangle”)

Countably infinite.

Same size as the natural numbers!!
Pairs of natural numbers.

Enumerate in list:
(0, 0), (1, 0), (0, 1), (2, 0), (1, 1), (0, 2), …

The pair (a, b), is in first 
(a + b + 1)(a + b)/2 elements of list!

(i.e., “triangle”).

Countably infinite.
Same size as the natural numbers!!
Pairs of natural numbers.

Enumerate in list:

(0, 0), (1, 0), (0, 1), (2, 0), (1, 1), (0, 2), ……
Pairs of natural numbers.

Enumerate in list:
(0,0), (1,0), (0,1), (2,0), (1,1), (0,2), ……
Pairs of natural numbers.

Enumerate in list:
(0, 0), (1, 0), (0, 1), (2, 0), (1, 1), (0, 2), ……

The pair \((a, b)\), is in first \((a + b + 1)(a + b) / 2\) elements of list!

(i.e., “triangle”).

Countably infinite.

Same size as the natural numbers!!
Pairs of natural numbers.

Enumerate in list:

\[(0, 0), (1, 0), (0, 1), (2, 0), (1, 1), (0, 2), \ldots\]
Pairs of natural numbers.

Enumerate in list:
(0,0), (1,0), (0,1), (2,0), (1,1), (0,2), ……

The pair \((a, b)\), is in first \((a + b + 1)(a + b)/2\) elements of list! (i.e., “triangle”).

Countably infinite.

Same size as the natural numbers!!
Pairs of natural numbers.

Enumerate in list:
(0,0), (1,0), (0,1), (2,0), (1,1), (0,2), …

The pair \((a, b)\), is in first \((a + b + 1)(a + b)/2\) elements of list!
Pairs of natural numbers.

Enumerate in list:
(0, 0), (1, 0), (0, 1), (2, 0), (1, 1), (0, 2), …

The pair \((a, b)\), is in first \((a + b + 1)(a + b)/2\) elements of list! (i.e., “triangle”).
Pairs of natural numbers.

Enumerate in list:
$(0,0), (1,0), (0,1), (2,0), (1,1), (0,2), \ldots$.

The pair $(a, b)$ is in first $(a+b+1)(a+b)/2$ elements of list! (i.e., “triangle”).

Countably infinite.
Pairs of natural numbers.

Enumerate in list:
(0,0), (1,0), (0,1), (2,0), (1,1), (0,2), …

The pair \((a, b)\), is in first \((a + b + 1)(a + b)/2\) elements of list!
(i.e., “triangle”).

Countably infinite.

Same size as the natural numbers!!
Rationals?

Positive rational number.
Rationals?

Positive rational number.
Lowest terms: $a/b$
Rationals?

Positive rational number.
Lowest terms: \( \frac{a}{b} \)
\( a, b \in N \)
Positive rational number.
Lowest terms: $a/b$
$a, b \in N$
with $gcd(a, b) = 1$. 

The rationals are countably infinite.
Rationals?

Positive rational number.
Lowest terms: \( a/b \)
\( a, b \in \mathbb{N} \)
with \( \gcd(a, b) = 1 \).

Infinite subset of \( \mathbb{N} \times \mathbb{N} \).
Positive rational number.
Lowest terms: $a/b$
$a, b \in \mathbb{N}$
with $gcd(a, b) = 1$.
Infinite subset of $\mathbb{N} \times \mathbb{N}$.
Countably infinite!
Rationals?

Positive rational number.
Lowest terms: $a/b$
$a, b \in N$
with $gcd(a, b) = 1$.

Infinite subset of $N \times N$.

Countably infinite!

All rational numbers?
Positive rational number.
Lowest terms: $a/b$
$a, b \in \mathbb{N}$
with $gcd(a, b) = 1$.

Infinite subset of $\mathbb{N} \times \mathbb{N}$.

Countably infinite!

All rational numbers?

Negative rationals are countable.
Rationals?

Positive rational number.  
Lowest terms: $a/b \quad a, b \in N$  
with $gcd(a, b) = 1$.

Infinite subset of $N \times N$.

Countably infinite!

All rational numbers?

Negative rationals are countable. (Same size as positive rationals.)
Rationals?

Positive rational number.
Lowest terms: \(a/b\)
\(a, b \in N\)
with \(gcd(a, b) = 1\).

Infinite subset of \(N \times N\).

Countably infinite!

All rational numbers?

Negative rationals are countable. (Same size as positive rationals.)

Put all rational numbers in a list.
Rationals?

Positive rational number.
Lowest terms: \( a/b \)
\( a, b \in N \)
with \( gcd(a, b) = 1 \).

Infinite subset of \( N \times N \).

Countably infinite!

All rational numbers?

Negative rationals are countable. (Same size as positive rationals.)
Put all rational numbers in a list.
First negative, then nonegative
Positive rational number.
Lowest terms: \( a/b \)
\( a, b \in N \)
with \( \gcd(a, b) = 1 \).

Infinite subset of \( N \times N \).

Countably infinite!

All rational numbers?

Negative rationals are countable. (Same size as positive rationals.)

Put all rational numbers in a list.

First negative, then nonegative ???
Rationals?

Positive rational number. 
Lowest terms: $a/b$

$a, b \in N$

with $gcd(a, b) = 1$.

Infinite subset of $N \times N$.

Countably infinite!

All rational numbers?

Negative rationals are countable. (Same size as positive rationals.)

Put all rational numbers in a list.

First negative, then nonegative ??? No!
Rationals?

Positive rational number.
Lowest terms: \(a/b\)
\(a, b \in \mathbb{N}\)
with \(gcd(a, b) = 1\).

Infinite subset of \(\mathbb{N} \times \mathbb{N}\).
Countably infinite!

All rational numbers?
Negative rationals are countable. (Same size as positive rationals.)

Put all rational numbers in a list.
First negative, then nonegative ??? No!
Repeatedly and alternatively take one from each list.
Positive rational number.  
Lowest terms: $a/b$  
$a, b \in \mathbb{N}$  
with $gcd(a, b) = 1$.  

Infinite subset of $\mathbb{N} \times \mathbb{N}$.  
Countably infinite!

All rational numbers?  

Negative rationals are countable. (Same size as positive rationals.)  

Put all rational numbers in a list.  

First negative, then nonegative ??? No!  

Repeatedly and alternatively take one from each list.  
Interleave Streams in 61A
Rationals?

Positive rational number.
Lowest terms: \( a/b \)
\( a, b \in N \)
with \( \gcd(a, b) = 1 \).

Infinite subset of \( N \times N \).
Countably infinite!

All rational numbers?
Negative rationals are countable. (Same size as positive rationals.)

Put all rational numbers in a list.
First negative, then nonegative ??? No!
Repeatedly and alternatively take one from each list.
Interleave Streams in 61A

The rationals are countably infinite.
Real numbers are same size as integers?
Are the set of reals countable?
The reals.

Are the set of reals countable?

Let's consider the reals \([0, 1]\).
The reals.

Are the set of reals countable?

Let's consider the reals \([0, 1]\).

Each real has a decimal representation.
The reals.

Are the set of reals countable?

Let's consider the reals $[0, 1]$.

Each real has a decimal representation.

.5000000000...
Are the set of reals countable?

Lets consider the reals [0, 1].

Each real has a decimal representation.

.5000000000... (1/2)
Are the set of reals countable?

Let's consider the reals $[0, 1]$.

Each real has a decimal representation.

.500000000... (1/2)
.785398162...
The reals.

Are the set of reals countable?

Let's consider the reals $[0, 1]$.

Each real has a decimal representation.

$.500000000...$ (1/2)

$.785398162...$ $\pi/4$
The reals.

Are the set of reals countable?

Let's consider the reals \([0, 1]\).

Each real has a decimal representation.

0.500000000... (1/2)

0.785398162... \(\pi/4\)

0.367879441...
Are the set of reals countable?

Let's consider the reals \([0, 1]\).

Each real has a decimal representation.
- \(.500000000...\) \((1/2)\)
- \(.785398162...\) \(\pi/4\)
- \(.367879441...\) \(1/e\)
The reals.

Are the set of reals countable?

Let's consider the reals $[0, 1]$.

Each real has a decimal representation.

- $0.500000000\ldots$ (1/2)
- $0.785398162\ldots$ $\pi/4$
- $0.367879441\ldots$ $1/e$
- $0.632120558\ldots$
Are the set of reals countable?

Let's consider the reals $[0, 1]$.

Each real has a decimal representation.

\[ \ldots \] (1/2)  
\[ \ldots \pi/4 \]  
\[ \ldots 1/e \]  
\[ \ldots 1 - 1/e \]
Are the set of reals countable?

Let's consider the reals $[0, 1]$.

Each real has a decimal representation.

- $0.500000000\ldots$ (1/2)
- $0.785398162\ldots$ $\pi/4$
- $0.367879441\ldots$ $1/e$
- $0.632120558\ldots$ $1 - 1/e$
- $0.345212312\ldots$
Are the set of reals countable?

Let's consider the reals \([0, 1]\).

Each real has a decimal representation.

- 0.500000000... \((1/2)\)
- 0.785398162... \(\pi/4\)
- 0.367879441... \(1/e\)
- 0.632120558... \(1 - 1/e\)
- 0.345212312... Some real number
Are the set of reals countable?

Let's consider the reals $[0, 1]$.

Each real has a decimal representation.
- $0.500000000... \ (1/2)$
- $0.785398162... \ \pi/4$
- $0.367879441... \ 1/e$
- $0.632120558... \ 1 - 1/e$
- $0.345212312... \ $ Some real number
Diagonalization.

If countable, there a listing, $L$ contains all reals.
Diagonalization.

If countable, there a listing, $L$ contains all reals. For example
Diagonalization.

If countable, there a listing, $L$ contains all reals. For example
0: .5000000000...
Diagonalization.

If countable, there a listing, $L$ contains all reals. For example

0: .500000000...
1: .785398162...
Diagonalization.

If countable, there a listing, \( L \) contains all reals. For example

0: \( .500000000... \)
1: \( .785398162... \)
2: \( .367879441... \)
Diagonalization.

If countable, there a listing, $L$ contains all reals. For example

0: .5000000000...
1: .785398162...
2: .367879441...
3: .632120558...

Construct "diagonal" number: .7767...

Diagonal Number:

Digit $i$ is 7 if number $i$'s $i$th digit is not 7 and 6 otherwise.

Diagonal number for a list differs from every number in list!

Diagonal number not in list.

Diagonal number is real.

Contradiction!

Subset $[0, 1]$ is not countable!!
Diagonalization.

If countable, there a listing, $L$ contains all reals. For example

0: .500000000...
1: .785398162...
2: .367879441...
3: .632120558...
4: .345212312...
Diagonalization.

If countable, there a listing, $L$ contains all reals. For example

0: .500000000...
1: .785398162...
2: .367879441...
3: .632120558...
4: .345212312...

...
Diagonalization.

If countable, there a listing, $L$ contains all reals. For example

0: .500000000...
1: .785398162...
2: .367879441...
3: .632120558...
4: .345212312...

Construct “diagonal” number:
Diagonalization.

If countable, there a listing, \( L \) contains all reals. For example

0: \( .5000000000... \)
1: \( .785398162... \)
2: \( .367879441... \)
3: \( .632120558... \)
4: \( .345212312... \)

Construct “diagonal” number: .7
Diagonalization.

If countable, there a listing, \( L \) contains all reals. For example

0: \( .500000000... \)
1: \( .785398162... \)
2: \( .367879441... \)
3: \( .632120558... \)
4: \( .345212312... \)

Construct “diagonal” number: \( .77 \)
Diagonalization.

If countable, there a listing, \( L \) contains all reals. For example

0: \[.500000000\ldots\]
1: \[.785398162\ldots\]
2: \[.367879441\ldots\]
3: \[.632120558\ldots\]
4: \[.345212312\ldots\]

Construct “diagonal” number: \[.776\]
Diagonalization.

If countable, there a listing, \( L \) contains all reals. For example

0: \(.500000000...\)
1: \(.785398162...\)
2: \(.367879441...\)
3: \(.632120558...\)
4: \(.345212312...\)

Construct “diagonal” number: \(.7767\)
Diagonalization.

If countable, there a listing, \( L \) contains all reals. For example

0: \(.5000000000\ldots\)
1: \(.785398162\ldots\)
2: \(.367879441\ldots\)
3: \(.632120558\ldots\)
4: \(.345212312\ldots\)

Construct “diagonal” number: \(.77677\)
Diagonalization.

If countable, there a listing, \( L \) contains all reals. For example

0: .500000000...
1: .785398162...
2: .367879441...
3: .632120558...
4: .345212312...

::

Construct “diagonal” number: .77677…
Diagonalization.

If countable, there a listing, $L$ contains all reals. For example

0: .5000000000...
1: .785398162...
2: .367879441...
3: .632120558...
4: .345212312...

Construct “diagonal” number: .77677…

Diagonal Number:
Diagonalization.

If countable, there a listing, \( L \) contains all reals. For example

0: .5000000000...
1: .785398162...
2: .367879441...
3: .632120558...
4: .345212312...
...

Construct “diagonal” number: .77677...

Diagonal Number: Digit \( i \) is 7 if number \( i \)’s \( i \)th digit is not 7
Diagonalization.

If countable, there a listing, \( L \) contains all reals. For example

0: \( .5000000000... \)
1: \( .785398162... \)
2: \( .367879441... \)
3: \( .632120558... \)
4: \( .345212312... \)

: 

Construct “diagonal” number: \( .77677... \)

Diagonal Number: Digit \( i \) is 7 if number \( i \)’s \( i \)th digit is not 7 and 6 otherwise.
Diagonalization.

If countable, there a listing, $L$ contains all reals. For example

0: $0.5000000000...$
1: $0.785398162...$
2: $0.367879441...$
3: $0.632120558...$
4: $0.345212312...$

Construct “diagonal” number: $0.77677...$

Diagonal Number: Digit $i$ is 7 if number $i$’s $i$th digit is not 7 and 6 otherwise.

Diagonal number for a list differs from every number in list!
Diagonalization.

If countable, there a listing, \( L \) contains all reals. For example

0: \(.500000000...\)
1: \(.785398162...\)
2: \(.367879441...\)
3: \(.632120558...\)
4: \(.345212312...\)

...

Construct “diagonal” number: \(.77677...\)

Diagonal Number: Digit \( i \) is 7 if number \( i \)’s \( i \)th digit is not 7 and 6 otherwise.

Diagonal number for a list differs from every number in list! Diagonal number not in list.
Diagonalization.

If countable, there a listing, \( L \) contains all reals. For example

0: \(.500000000\ldots\)

1: \(.785398162\ldots\)

2: \(.367879441\ldots\)

3: \(.632120558\ldots\)

4: \(.345212312\ldots\)

: 

Construct “diagonal” number: \(.77677\ldots\)

Diagonal Number: Digit \( i \) is 7 if number \( i \)’s \( i \)th digit is not 7 and 6 otherwise.

Diagonal number for a list differs from every number in list!

Diagonal number not in list.

Diagonal number is real.
Diagonalization.

If countable, there a listing, \( L \) contains all reals. For example

0: .500000000...
1: .785398162...
2: .367879441...
3: .632120558...
4: .345212312...
...

Construct “diagonal” number: .77677...

Diagonal Number: Digit \( i \) is 7 if number \( i \)’s \( i \)th digit is not 7 and 6 otherwise.

Diagonal number for a list differs from every number in list!

Diagonal number not in list.

Diagonal number is real.

Contradiction!
Diagonalization.

If countable, there a listing, \( L \) contains all reals. For example

0: \( .500000000... \)
1: \( .785398162... \)
2: \( .367879441... \)
3: \( .632120558... \)
4: \( .345212312... \)

:  

Construct “diagonal” number: \( .77677... \)

Diagonal Number: Digit \( i \) is 7 if number \( i \)'s \( i \)th digit is not 7 and 6 otherwise.

Diagonal number for a list differs from every number in list! Diagonal number not in list.

Diagonal number is real.

Contradiction!

Subset \([0, 1]\) is not countable!!
All reals?

Subset $[0,1]$ is not countable!!
All reals?

Subset [0, 1] is not countable!!

What about all reals?
All reals?

Subset [0, 1] is not countable!!
What about all reals?
No.
All reals?

Subset [0, 1] is not countable!!
What about all reals?
No.
Any subset of a countable set is countable.
All reals?

Subset $[0, 1]$ is not countable!!

What about all reals?
No.

Any subset of a countable set is countable.

If reals are countable then so is $[0, 1]$. 
Diagonalization.

1. Assume that a set $S$ can be enumerated.
**Diagonalization.**

1. Assume that a set $S$ can be enumerated.

2. Consider an arbitrary list of all the elements of $S$. 
1. Assume that a set $S$ can be enumerated.
2. Consider an arbitrary list of all the elements of $S$.
3. Use the diagonal from the list to construct a new element $t$. 

Diagonalization.

1. Assume that a set $S$ can be enumerated.
2. Consider an arbitrary list of all the elements of $S$.
3. Use the diagonal from the list to construct a new element $t$.
4. Show that $t$ is different from all elements in the list.
5. Show that $t$ is in $S$.
6. Contradiction.
Diagonalization.

1. Assume that a set $S$ can be enumerated.
2. Consider an arbitrary list of all the elements of $S$.
3. Use the diagonal from the list to construct a new element $t$.
4. Show that $t$ is different from all elements in the list $\implies t$ is not in the list.
1. Assume that a set $S$ can be enumerated.

2. Consider an arbitrary list of all the elements of $S$.

3. Use the diagonal from the list to construct a new element $t$.

4. Show that $t$ is different from all elements in the list $\Rightarrow t$ is not in the list.

5. Show that $t$ is in $S$.

Contradiction.
Diagonalization.

1. Assume that a set $S$ can be enumerated.
2. Consider an arbitrary list of all the elements of $S$.
3. Use the diagonal from the list to construct a new element $t$.
4. Show that $t$ is different from all elements in the list
   $\implies t$ is not in the list.
5. Show that $t$ is in $S$.
6. Contradiction.
Another diagonalization.

The set of all subsets of $N$. 
Another diagonalization.

The set of all subsets of \( N \).

Example subsets of \( N \): \( \{0\}, \)
Another diagonalization.

The set of all subsets of $\mathbb{N}$.

Example subsets of $\mathbb{N}$: $\{0\}$, $\{0, \ldots, 7\}$,
Another diagonalization.

The set of all subsets of $N$.

Example subsets of $N$: $\{0\}$, $\{0,\ldots,7\}$,
Another diagonalization.

The set of all subsets of \( N \).

Example subsets of \( N \): \{0\}, \{0,\ldots,7\}, evens,
Another diagonalization.

The set of all subsets of $N$.

Example subsets of $N$: \{0\}, \{0, \ldots, 7\},
evens, odds,
Another diagonalization.

The set of all subsets of $\mathbb{N}$.

Example subsets of $\mathbb{N}$: $\{0\}$, $\{0, \ldots, 7\}$, evens, odds, primes,
Another diagonalization.

The set of all subsets of $N$.

Example subsets of $N$: $\{0\}$, $\{0, \ldots, 7\}$, evens, odds, primes,
Another diagonalization.

The set of all subsets of \( N \).

Example subsets of \( N \): \( \{0\} \), \( \{0,\ldots,7\} \),
evens, odds, primes,

Assume is countable.
Another diagonalization.

The set of all subsets of \( N \).

Example subsets of \( N \): \( \{0\} \), \( \{0,\ldots,7\} \), evens, odds, primes,

Assume is countable.

There is a listing, \( L \), that contains all subsets of \( N \).
Another diagonalization.

The set of all subsets of $N$.

Example subsets of $N$: $\{0\}$, $\{0, \ldots, 7\}$, evens, odds, primes,

Assume is countable.

There is a listing, $L$, that contains all subsets of $N$.

Define a diagonal set, $D$:
Another diagonalization.

The set of all subsets of $N$.

Example subsets of $N$: $\{0\}$, $\{0, \ldots, 7\}$, evens, odds, primes,

Assume is countable.

There is a listing, $L$, that contains all subsets of $N$.

Define a diagonal set, $D$:
If $i$th set in $L$ does not contain $i$, $i \in D$.
Another diagonalization.

The set of all subsets of $N$.

Example subsets of $N$: $\{0\}$, $\{0, \ldots, 7\}$, evens, odds, primes,

Assume is countable.

There is a listing, $L$, that contains all subsets of $N$.

Define a diagonal set, $D$:
If $i$th set in $L$ does not contain $i$, $i \in D$.
otherwise $i \notin D$.

$D$ is different from $i$th set in $L$ for every $i$.
$D$ is a subset of $N$.
$L$ does not contain all subsets of $N$.

Contradiction.

Theorem: The set of all subsets of $N$ is not countable.

(The set of all subsets of $S$, is the powerset of $N$.)
Another diagonalization.

The set of all subsets of $N$.

Example subsets of $N$: $\{0\}$, $\{0, \ldots, 7\}$,
evens, odds, primes,

Assume is countable.

There is a listing, $L$, that contains all subsets of $N$.

Define a diagonal set, $D$:
If $i$th set in $L$ does not contain $i$, $i \in D$.
otherwise $i \notin D$.
Another diagonalization.

The set of all subsets of $N$.

Example subsets of $N$: $\{0\}$, $\{0, \ldots, 7\}$, evens, odds, primes,

Assume is countable.

There is a listing, $L$, that contains all subsets of $N$.

Define a diagonal set, $D$:
If $i$th set in $L$ does not contain $i$, $i \in D$.
otherwise $i \notin D$.

$D$ is different from $i$th set in $L$ for every $i$.
Another diagonalization.

The set of all subsets of $N$.

Example subsets of $N$: $\{0\}$, $\{0,\ldots,7\}$, evens, odds, primes,

Assume is countable.

There is a listing, $L$, that contains all subsets of $N$.

Define a diagonal set, $D$:
If $i$th set in $L$ does not contain $i$, $i \in D$.
otherwise $i \notin D$.

$D$ is different from $i$th set in $L$ for every $i$.
$\implies D$ is not in the listing.
Another diagonalization.

The set of all subsets of $N$.

Example subsets of $N$: \{0\}, \{0,\ldots,7\},
evens, odds, primes,

Assume is countable.

There is a listing, $L$, that contains all subsets of $N$.

Define a diagonal set, $D$:

If $i$th set in $L$ does not contain $i$, $i \in D$.
otherwise $i \not\in D$.

$D$ is different from $i$th set in $L$ for every $i$.

$\implies D$ is not in the listing.

$D$ is a subset of $N$. 
Another diagonalization.

The set of all subsets of \( N \).

Example subsets of \( N \): \( \{0\} \), \( \{0, \ldots, 7\} \), evens, odds, primes,

Assume is countable.

There is a listing, \( L \), that contains all subsets of \( N \).

Define a diagonal set, \( D \):
If \( i \)th set in \( L \) does not contain \( i \), \( i \in D \).
otherwise \( i \notin D \).

\( D \) is different from \( i \)th set in \( L \) for every \( i \).
\( \Rightarrow \) \( D \) is not in the listing.

\( D \) is a subset of \( N \).

\( L \) does not contain all subsets of \( N \).
Another diagonalization.

The set of all subsets of $N$.

Example subsets of $N$: $\{0\}$, $\{0, \ldots, 7\}$, evens, odds, primes,

Assume is countable.

There is a listing, $L$, that contains all subsets of $N$.

Define a diagonal set, $D$:
If $i$th set in $L$ does not contain $i$, $i \in D$.
otherwise $i \notin D$.

$D$ is different from $i$th set in $L$ for every $i$.
$\implies D$ is not in the listing.

$D$ is a subset of $N$.

$L$ does not contain all subsets of $N$.

Contradiction.
Another diagonalization.

The set of all subsets of \( N \).

Example subsets of \( N \): \( \{0\}, \{0, \ldots, 7\} \), evens, odds, primes,

Assume is countable.

There is a listing, \( L \), that contains all subsets of \( N \).

Define a diagonal set, \( D \):
If \( i \)th set in \( L \) does not contain \( i \), \( i \in D \).
otherwise \( i \notin D \).

\( D \) is different from \( i \)th set in \( L \) for every \( i \).
\( \implies D \) is not in the listing.

\( D \) is a subset of \( N \).

\( L \) does not contain all subsets of \( N \).

Contradiction.

**Theorem:** The set of all subsets of \( N \) is not countable.
Another diagonalization.

The set of all subsets of $N$.

Example subsets of $N$: $\{0\}$, $\{0, \ldots, 7\}$, evens, odds, primes,

Assume is countable.

There is a listing, $L$, that contains all subsets of $N$.

Define a diagonal set, $D$:
If $i$th set in $L$ does not contain $i$, $i \in D$.
otherwise $i \notin D$.

$D$ is different from $i$th set in $L$ for every $i$.
$\implies D$ is not in the listing.

$D$ is a subset of $N$.

$L$ does not contain all subsets of $N$.

Contradiction.

**Theorem:** The set of all subsets of $N$ is not countable. (The set of all subsets of $S$, is the powerset of $N$.)
Diagonalize Natural Number.

Natural numbers have a listing, $L$. 

Make a diagonal number, $D$: differ from $i$th element of $L$ in $i$th digit. Differs from all elements of listing. $D$ is a natural number... Not. 

Any natural number has a finite number of digits. "Construction" requires an infinite number of digits.
Diagonalize Natural Number.

Natural numbers have a listing, $L$.

Make a diagonal number, $D$:

differ from $i$th element of $L$ in $i$th digit.
Natural numbers have a listing, $L$.

Make a diagonal number, $D$:  

differ from $i$th element of $L$ in $i$th digit.

Differs from all elements of listing.
Diagonalize Natural Number.

Natural numbers have a listing, $L$.

Make a diagonal number, $D$:

differ from $i$th element of $L$ in $i$th digit.

Differs from all elements of listing.

$D$ is a natural number...
Diagonalize Natural Number.

Natural numbers have a listing, $L$.

Make a diagonal number, $D$:

differ from $i$th element of $L$ in $i$th digit.

Differs from all elements of listing.

$D$ is a natural number... Not.
Diagonalize Natural Number.

Natural numbers have a listing, $L$.

Make a diagonal number, $D$:

differ from $i$th element of $L$ in $i$th digit.

Differs from all elements of listing.

$D$ is a natural number... Not.

Any natural number has a finite number of digits.
Diagonalize Natural Number.

Natural numbers have a listing, $L$.

Make a diagonal number, $D$:

differ from $i$th element of $L$ in $i$th digit.

Differs from all elements of listing.

$D$ is a natural number... Not.

Any natural number has a finite number of digits.

“Construction” requires an infinite number of digits.
The Continuum hypothesis.

There is no set with cardinality between the naturals and the reals.
The Continuum hypothesis.

There is no set with cardinality between the naturals and the reals. First of Hilbert’s problems!
Cardinalities of uncountable sets?

Cardinality of $[0, 1]$ smaller than all the reals?
Cardinalities of uncountable sets?

Cardinality of $[0, 1]$ smaller than all the reals?

$f : \mathbb{R}^+ \rightarrow [0, 1]$. 

One to one.

If both in $[0, \frac{1}{2})$, a shift $\Rightarrow f(x) \neq f(y)$.

If neither in $[0, \frac{1}{2})$, a division $\Rightarrow f(x) \neq f(y)$.

If one is in $[0, \frac{1}{2})$ and one isn't, different ranges $\Rightarrow f(x) \neq f(y)$.

Bijection!

$[0, 1]$ is same cardinality as nonnegative reals!
Cardinalities of uncountable sets?

Cardinality of $[0, 1]$ smaller than all the reals?

$f : \mathbb{R}^+ \rightarrow [0, 1]$.

$$f(x) = \begin{cases} 
  x + \frac{1}{2} & \text{if } 0 \leq x \leq 1/2 \\
  \frac{1}{4x} & \text{if } x > 1/2 
\end{cases}$$
Cardinalities of uncountable sets?

Cardinality of $[0, 1]$ smaller than all the reals?

$f : \mathbb{R}^+ \to [0, 1]$.

$$f(x) = \begin{cases} 
  x + \frac{1}{2} & 0 \leq x \leq 1/2 \\
  \frac{1}{4x} & x > 1/2
\end{cases}$$

One to one.
Cardinalities of uncountable sets?

Cardinality of $[0, 1]$ smaller than all the reals?

$f : \mathbb{R}^+ \rightarrow [0, 1]$.

$$f(x) = \begin{cases} 
  x + \frac{1}{2} & 0 \leq x \leq \frac{1}{2} \\
  \frac{1}{4x} & x > \frac{1}{2}
\end{cases}$$

One to one. $x \neq y$
Cardinalities of uncountable sets?

Cardinality of \([0, 1]\) smaller than all the reals?

\(f : \mathbb{R}^+ \rightarrow [0, 1].\)

\[
f(x) = \begin{cases} 
  x + \frac{1}{2} & \text{if } 0 \leq x \leq 1/2 \\
  \frac{1}{4x} & \text{if } x > 1/2 
\end{cases}
\]

One to one. \(x \neq y\)

If both in \([0, 1/2],\)
Cardinalities of uncountable sets?

Cardinality of $[0, 1]$ smaller than all the reals?

$f : R^+ \rightarrow [0, 1].$

$$f(x) = \begin{cases} 
    x + \frac{1}{2} & \text{if } 0 \leq x \leq 1/2 \\
    \frac{1}{4x} & \text{if } x > 1/2 
\end{cases}$$

One to one. $x \neq y$

If both in $[0, 1/2]$, a shift
Cardinalities of uncountable sets?

Cardinality of $[0, 1]$ smaller than all the reals?

$f : \mathbb{R}^+ \rightarrow [0, 1]$.

$$f(x) = \begin{cases} 
  x + \frac{1}{2} & 0 \leq x \leq 1/2 \\
  \frac{1}{4x} & x > 1/2 
\end{cases}$$

One to one. $x \neq y$

If both in $[0, 1/2]$, a shift $\implies f(x) \neq f(y)$. 
Cardinalities of uncountable sets?

Cardinality of $[0, 1]$ smaller than all the reals?

$f : \mathbb{R}^+ \to [0, 1]$. 

$$f(x) = \begin{cases} 
  x + \frac{1}{2} & 0 \leq x \leq \frac{1}{2} \\
  \frac{1}{4x} & x > \frac{1}{2}
\end{cases}$$

One to one. $x \neq y$

If both in $[0, 1/2]$, a shift $\implies f(x) \neq f(y)$.
If neither in $[0, 1/2]$
Cardinalities of uncountable sets?

Cardinality of $[0, 1]$ smaller than all the reals?

$f : R^+ \rightarrow [0, 1]$.

$$f(x) = \begin{cases} 
  x + \frac{1}{2} & 0 \leq x \leq 1/2 \\
  \frac{1}{4x} & x > 1/2 
\end{cases}$$

One to one. $x \neq y$

If both in $[0, 1/2]$, a shift $\implies f(x) \neq f(y)$.

If neither in $[0, 1/2]$ a division
Cardinalities of uncountable sets?

Cardinality of $[0, 1]$ smaller than all the reals?

$f : \mathbb{R}^+ \rightarrow [0, 1]$.

$$f(x) = \begin{cases} 
  x + \frac{1}{2} & 0 \leq x \leq \frac{1}{2} \\
  \frac{1}{4x} & x > \frac{1}{2} 
\end{cases}$$

One to one. $x \neq y$

If both in $[0, 1/2]$, a shift $\implies f(x) \neq f(y)$.

If neither in $[0, 1/2]$ a division $\implies f(x) \neq f(y)$.
Cardinalities of uncountable sets?

Cardinality of $[0, 1]$ smaller than all the reals?

$f : R^+ \rightarrow [0, 1]$. 

$$f(x) = \begin{cases} 
  x + \frac{1}{2} & 0 \leq x \leq 1/2 \\
  \frac{1}{4x} & x > 1/2 
\end{cases}$$

One to one. $x \neq y$

If both in $[0, 1/2]$, a shift $\implies f(x) \neq f(y)$.

If neither in $[0, 1/2]$ a division $\implies f(x) \neq f(y)$.

If one is in $[0, 1/2]$ and one isn’t,
Cardinalities of uncountable sets?

Cardinality of $[0, 1]$ smaller than all the reals?

$f : R^+ \rightarrow [0, 1]$. 

$$f(x) = \begin{cases} 
  x + \frac{1}{2} & 0 \leq x \leq 1/2 \\
  \frac{1}{4x} & x > 1/2 
\end{cases}$$

One to one. $x \neq y$

If both in $[0, 1/2]$, a shift $\implies f(x) \neq f(y)$.

If neither in $[0, 1/2]$ a division $\implies f(x) \neq f(y)$.

If one is in $[0, 1/2]$ and one isn’t, different ranges
Cardinalities of uncountable sets?

Cardinality of $[0, 1]$ smaller than all the reals?

$f : R^+ \to [0, 1]$.

$$f(x) = \begin{cases} 
  x + \frac{1}{2} & 0 \leq x \leq 1/2 \\
  \frac{1}{4x} & x > 1/2 
\end{cases}$$

One to one. $x \neq y$

If both in $[0, 1/2]$, a shift $\implies f(x) \neq f(y)$.

If neither in $[0, 1/2]$ a division $\implies f(x) \neq f(y)$.

If one is in $[0, 1/2]$ and one isn’t, different ranges $\implies f(x) \neq f(y)$. 
Cardinalities of uncountable sets?

Cardinality of \([0, 1]\) smaller than all the reals?

\[ f : R^+ \rightarrow [0, 1]. \]

\[ f(x) = \begin{cases} 
  x + \frac{1}{2} & 0 \leq x \leq 1/2 \\
  \frac{1}{4x} & x > 1/2 
\end{cases} \]

One to one. \( x \neq y \)

If both in \([0, 1/2]\), a shift \( \implies f(x) \neq f(y) \).
If neither in \([0, 1/2]\) a division \( \implies f(x) \neq f(y) \).
If one is in \([0, 1/2]\) and one isn’t, different ranges \( \implies f(x) \neq f(y) \).

Bijection!
Cardinalities of uncountable sets?

Cardinality of \([0, 1]\) smaller than all the reals?

\[ f : R^+ \rightarrow [0, 1]. \]

\[ f(x) = \begin{cases} 
  x + \frac{1}{2} & 0 \leq x \leq 1/2 \\
  \frac{1}{4x} & x > 1/2 
\end{cases} \]

One to one. \( x \neq y \)

If both in \([0, 1/2]\), a shift \(\implies f(x) \neq f(y)\).

If neither in \([0, 1/2]\) a division \(\implies f(x) \neq f(y)\).

If one is in \([0, 1/2]\) and one isn’t, different ranges \(\implies f(x) \neq f(y)\).

Bijection!

\([0, 1]\) is same cardinality as nonnegative reals!
Generalized Continuum hypothesis.

There is no infinite set whose cardinality is between the cardinality of an infinite set and its power set.
Generalized Continuum hypothesis.

There is no infinite set whose cardinality is between the cardinality of an infinite set and its power set.

The powerset of a set is the set of all subsets.
Resolution of hypothesis?

Gődel. 1940.

Can't use math!

If math doesn't contain a contradiction.

This statement is a lie.

Is the statement above true?

The barber shaves every person who does not shave themselves.

Who shaves the barber?

Self reference.
Resolution of hypothesis?

Gödel. 1940.
Can’t use math!
Gödel. 1940.
Can’t use math!
If math doesn’t contain a contradiction.
Resolution of hypothesis?

Gödel. 1940.
Can’t use math!
If math doesn’t contain a contradiction.
This statement is a lie.
Resolution of hypothesis?

Gödel. 1940.
Can’t use math!
If math doesn’t contain a contradiction.

This statement is a lie.

Is the statement above true?
Resolution of hypothesis?

Gödel. 1940.
Can't use math!
If math doesn't contain a contradiction.
This statement is a lie.

Is the statement above true?
The barber shaves every person who does not shave themselves.
Gödel. 1940.
Can’t use math!
If math doesn’t contain a contradiction.
This statement is a lie.

Is the statement above true?

The barber shaves every person who does not shave themselves.

Who shaves the barber?
Resolution of hypothesis?

Gödel. 1940.
Can’t use math!
If math doesn’t contain a contradiction.

This statement is a lie.

Is the statement above true?

The barber shaves every person who does not shave themselves.

Who shaves the barber?

Self reference.
More on...

...Tuesday..
More on...

...Tuesday..