Today.

Polynomials.
Polynomials.
Erasure Codes.
Today.

Polynomials.
Erasure Codes.
Error Correcting Codes.
Today.

Polynomials.
Erasure Codes.
Error Correcting Codes.
   Heads will explode.
Finite Fields

Modular Fact!!!
Finite Fields

Modular Fact!!!
Proof works for reals, rationals, and complex numbers.
Finite Fields

Modular Fact!!!
Proof works for reals, rationals, and complex numbers.
..but not for integers, since no multiplicative inverses.
Finite Fields

Modular Fact!!

Proof works for reals, rationals, and complex numbers.
..but not for integers, since no multiplicative inverses.
Arithmetic modulo a prime $p$ has multiplicative inverses..
Finite Fields

Modular Fact!!!
Proof works for reals, rationals, and complex numbers. 
..but not for integers, since no multiplicative inverses.
Arithmetic modulo a prime $p$ has multiplicative inverses..
..and has only a finite number of elements.
Finite Fields

Modular Fact!!!
Proof works for reals, rationals, and complex numbers..
..but not for integers, since no multiplicative inverses.
Arithmetic modulo a prime $p$ has multiplicative inverses..
..and has only a finite number of elements.
Good for computer science.
Finite Fields

Modular Fact!!!
Proof works for reals, rationals, and complex numbers.
..but not for integers, since no multiplicative inverses.
Arithmetic modulo a prime $p$ has multiplicative inverses..
..and has only a finite number of elements.
Good for computer science.
Arithmetic modulo a prime $m$ is a **finite field** denoted by $F_m$ or $GF(m)$. 

Modular Fact!!!
Proof works for reals, rationals, and complex numbers.
..but not for integers, since no multiplicative inverses.
Arithmetic modulo a prime $p$ has multiplicative inverses..
..and has only a finite number of elements.
Good for computer science.
Arithmetic modulo a prime $m$ is a finite field denoted by $F_m$ or $GF(m)$.
Intuitively, a field is a set with operations corresponding to addition, multiplication, and division.
Secret Sharing

**Modular Arithmetic Fact:** Exactly one polynomial degree \( \leq d \) over \( GF(p) \), \( P(x) \), that hits \( d + 1 \) points.
Secret Sharing

**Modular Arithmetic Fact:** Exactly one polynomial degree \( \leq d \) over \( GF(p) \), \( P(x) \), that hits \( d + 1 \) points.

**Shamir’s \( k \) out of \( n \) Scheme:**

1. Choose \( a_0 = s \), and randomly \( a_1, \ldots, a_{k-1} \).
2. Let \( P(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_0 \) with \( a_0 = s \).
3. Share \( i \) is point \((i, P(i) \mod p)\).

**Robustness:** Any \( k \) knows secret.
Knowing \( k \) pts, only one \( P(x) \), evaluate \( P(0) \).

**Secrecy:** Any \( k - 1 \) knows nothing.
Knowing \( \leq k - 1 \) pts, any \( P(0) \) is possible.
Secret Sharing

**Modular Arithmetic Fact:** Exactly one polynomial degree \( \leq d \) over \( GF(p) \), \( P(x) \), that hits \( d + 1 \) points.

**Shamir’s \( k \) out of \( n \) Scheme:**
Secret \( s \in \{0, \ldots, p - 1\} \)
Secret Sharing

**Modular Arithmetic Fact:** Exactly one polynomial degree $\leq d$ over $GF(p)$, $P(x)$, that hits $d+1$ points.

**Shamir’s $k$ out of $n$ Scheme:**
Secret $s \in \{0, \ldots, p-1\}$

1. Choose $a_0 = s$, and randomly $a_1, \ldots, a_{k-1}$. 


Secret Sharing

**Modular Arithmetic Fact:** Exactly one polynomial degree $\leq d$ over $GF(p)$, $P(x)$, that hits $d + 1$ points.

**Shamir’s $k$ out of $n$ Scheme:**
Secret $s \in \{0, \ldots, p - 1\}$

1. Choose $a_0 = s$, and randomly $a_1, \ldots, a_{k-1}$.
2. Let $P(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_0$ with $a_0 = s$. 
Secret Sharing

**Modular Arithmetic Fact:** Exactly one polynomial degree \( \leq d \) over \( GF(p) \), \( P(x) \), that hits \( d+1 \) points.

**Shamir’s \( k \) out of \( n \) Scheme:**
Secret \( s \in \{0, \ldots, p-1\} \)

1. Choose \( a_0 = s \), and randomly \( a_1, \ldots, a_{k-1} \).
2. Let \( P(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_0 \) with \( a_0 = s \).
3. Share \( i \) is point \((i, P(i) \mod p)\).
Secret Sharing

**Modular Arithmetic Fact:** Exactly one polynomial degree $\leq d$ over $GF(p)$, $P(x)$, that hits $d + 1$ points.

**Shamir’s $k$ out of $n$ Scheme:**
Secret $s \in \{0, \ldots, p - 1\}$

1. Choose $a_0 = s$, and randomly $a_1, \ldots, a_{k-1}$.
2. Let $P(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots a_0$ with $a_0 = s$.
3. Share $i$ is point $(i, P(i) \mod p)$.
Secret Sharing

**Modular Arithmetic Fact:** Exactly one polynomial degree $\leq d$ over $GF(p)$, $P(x)$, that hits $d + 1$ points.

**Shamir’s $k$ out of $n$ Scheme:**
Secret $s \in \{0, \ldots, p-1\}$

1. Choose $a_0 = s$, and randomly $a_1, \ldots, a_{k-1}$.
2. Let $P(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots a_0$ with $a_0 = s$.
3. Share $i$ is point $(i, P(i) \mod p)$.

**Robustness:** Any $k$ knows secret.
Secret Sharing

**Modular Arithmetic Fact:** Exactly one polynomial degree $\leq d$ over $GF(p)$, $P(x)$, that hits $d + 1$ points.

**Shamir’s $k$ out of $n$ Scheme:**
Secret $s \in \{0, \ldots, p - 1\}$

1. Choose $a_0 = s$, and randomly $a_1, \ldots, a_{k-1}$.
2. Let $P(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_0$ with $a_0 = s$.
3. Share $i$ is point $(i, P(i) \mod p)$.

**Robustness:** Any $k$ knows secret.
Knowing $k$ pts, only one $P(x)$, evaluate $P(0)$.

**Secrecy:** Any $k - 1$ knows nothing.
Secret Sharing

**Modular Arithmetic Fact:** Exactly one polynomial degree $\leq d$ over $GF(p)$, $P(x)$, that hits $d + 1$ points.

**Shamir’s $k$ out of $n$ Scheme:**
Secret $s \in \{0, \ldots, p - 1\}$

1. Choose $a_0 = s$, and randomly $a_1, \ldots, a_{k-1}$.
2. Let $P(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_0$ with $a_0 = s$.
3. Share $i$ is point $(i, P(i) \mod p)$.

**Roubusness:** Any $k$ knows secret. Knowing $k$ pts, only one $P(x)$, evaluate $P(0)$.

**Secrecy:** Any $k - 1$ knows nothing. Knowing $\leq k - 1$ pts, any $P(0)$ is possible.
Secret Sharing

Modular Arithmetic Fact: Exactly one polynomial degree \( \leq d \) over \( GF(p) \), \( P(x) \), that hits \( d + 1 \) points.

Shamir’s \( k \) out of \( n \) Scheme:
Secret \( s \in \{0, \ldots, p - 1\} \)

1. Choose \( a_0 = s \), and randomly \( a_1, \ldots, a_{k-1} \).
2. Let \( P(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_0 \) with \( a_0 = s \).
3. Share \( i \) is point \( (i, P(i) \mod p) \).

Roubustness: Any \( k \) knows secret.
Knowing \( k \) pts, only one \( P(x) \), evaluate \( P(0) \).
Secrecy: Any \( k - 1 \) knows nothing.
Knowing \( \leq k - 1 \) pts, any \( P(0) \) is possible.
Minimality.

Need $p > n$ to hand out $n$ shares: $P(1) \ldots P(n)$. 
Minimality.

Need $p > n$ to hand out $n$ shares: $P(1) \ldots P(n)$.

For an $b$-bit secret, must choose a prime $p > 2^b$. 
Minimality.

Need $p > n$ to hand out $n$ shares: $P(1) \ldots P(n)$.
For an $b$-bit secret, must choose a prime $p > 2^b$.

**Theorem:** There is always a prime between $n$ and $2n$. 
Minimality.

Need $p > n$ to hand out $n$ shares: $P(1) \ldots P(n)$.
For an $b$-bit secret, must choose a prime $p > 2^b$.

**Theorem:** There is always a prime between $n$ and $2n$.

Working over numbers within 1 bit of secret size. **Minimality.**
Minimality.

Need $p > n$ to hand out $n$ shares: $P(1) \ldots P(n)$.
For an $b$-bit secret, must choose a prime $p > 2^b$.

**Theorem:** There is always a prime between $n$ and $2n$.
Working over numbers within 1 bit of secret size. **Minimality.**
With $k$ shares, reconstruct polynomial, $P(x)$. 
Minimality.

Need $p > n$ to hand out $n$ shares: $P(1) \ldots P(n)$.
For an $b$-bit secret, must choose a prime $p > 2^b$.

Theorem: There is always a prime between $n$ and $2n$.

Working over numbers within 1 bit of secret size. Minimality.
With $k$ shares, reconstruct polynomial, $P(x)$.
With $k - 1$ shares, any of $p$ values possible for $P(0)$!
Minimality.

Need $p > n$ to hand out $n$ shares: $P(1) \ldots P(n)$.

For an $b$-bit secret, must choose a prime $p > 2^b$.

**Theorem:** There is always a prime between $n$ and $2n$.

Working over numbers within 1 bit of secret size. **Minimality.**

With $k$ shares, reconstruct polynomial, $P(x)$.

With $k - 1$ shares, any of $p$ values possible for $P(0)$!

(Almost) any $b$-bit string possible!
Minimality.

Need $p > n$ to hand out $n$ shares: $P(1) \ldots P(n)$. For an $b$-bit secret, must choose a prime $p > 2^b$.

**Theorem:** There is always a prime between $n$ and $2n$.

Working over numbers within 1 bit of secret size. **Minimality.**

With $k$ shares, reconstruct polynomial, $P(x)$.

With $k - 1$ shares, any of $p$ values possible for $P(0)$!

(Almost) any $b$-bit string possible!

(Almost) the same as what is missing: one $P(i)$.
Runtime.

1. Evaluate degree $k - 1$ polynomial $n$ times using $\log p$-bit numbers.
2. Reconstruct secret by solving system of $k$ equations using $\log p$-bit arithmetic.
Runtime.

Runtime: polynomial in $k$, $n$, and $\log p$.

1. Evaluate degree $k - 1$ polynomial $n$ times using $\log p$-bit numbers.

2. Reconstruct secret by solving system of $k$ equations using $\log p$-bit arithmetic.
A bit more counting.

What is the number of degree $d$ polynomials over $GF(m)$?

$m^d + 1$: $d + 1$ coefficients from $\{0, \ldots, m-1\}$.

$m^d + 1$: $d + 1$ points with $y$-values from $\{0, \ldots, m-1\}$.

Infinite number for reals, rationals, complex numbers!
A bit more counting.

What is the number of degree $d$ polynomials over $GF(m)$?

- $m^{d+1}$: $d + 1$ coefficients from $\{0, \ldots, m-1\}$. 

Infinite number for reals, rationals, complex numbers!
A bit more counting.

What is the number of degree $d$ polynomials over $GF(m)$?

$\quad m^{d+1}: d + 1$ coefficients from $\{0, \ldots, m - 1\}$.

$\quad m^{d+1}: d + 1$ points with $y$-values from $\{0, \ldots, m - 1\}$.
A bit more counting.

What is the number of degree $d$ polynomials over $GF(m)$?

- $m^{d+1}$: $d + 1$ coefficients from $\{0, \ldots, m-1\}$.
- $m^{d+1}$: $d + 1$ points with $y$-values from $\{0, \ldots, m-1\}$

Infinite number for reals, rationals, complex numbers!
Polynomials and Coding theory.
Erasure Codes.

Satellite

GPS device
Erasure Codes.

Satellite

GPS device

3 packet message.
Erasure Codes.

Satellite

3 packet message.

Lose 3 out 6 packets.

GPS device
Erasure Codes.

Satellite

3 packet message. So send 6!

1 2 3 1 2 3

Lose 3 out 6 packets.

GPS device
Erasure Codes.

Satellite

3 packet message. So send 6!

Lose 3 out 6 packets.
3 packet message. So send 6!

Lose 3 out 6 packets.

Erasure Codes.
Erasure Codes.

Satellite

3 packet message. So send 6!

Lose 3 out 6 packets.

GPS device

Gets packets 1, 1, and 3.
Solution Idea.

\( n \) packet message, channel that loses \( k \) packets.
Solution Idea.

$n$ packet message, channel that loses $k$ packets.
Must send $n + k$ packets!
Solution Idea.

\( n \) packet message, channel that loses \( k \) packets.
Must send \( n + k \) packets!

Any \( n \) packets
Solution Idea.

\( n \) packet message, channel that loses \( k \) packets.

Must send \( n + k \) packets!

Any \( n \) packets should allow reconstruction of \( n \) packet message.
Solution Idea.

$n$ packet message, channel that loses $k$ packets.
Must send $n + k$ packets!

- Any $n$ packets should allow reconstruction of $n$ packet message.
- Any $n$ point values
Solution Idea.

$n$ packet message, channel that loses $k$ packets.

Must send $n + k$ packets!

Any $n$ packets should allow reconstruction of $n$ packet message.

Any $n$ point values allow reconstruction of degree $n - 1$ polynomial.
Solution Idea.

$n$ packet message, channel that loses $k$ packets.
Must send $n + k$ packets!
   Any $n$ packets should allow reconstruction of $n$ packet message.
   Any $n$ point values allow reconstruction of degree $n - 1$ polynomial.
Alright!
Solution Idea.

\( n \) packet message, channel that loses \( k \) packets.
Must send \( n + k \) packets!

- Any \( n \) packets should allow reconstruction of \( n \) packet message.
- Any \( n \) point values allow reconstruction of degree \( n - 1 \) polynomial.

Alright!!
Solution Idea.

$n$ packet message, channel that loses $k$ packets.
Must send $n + k$ packets!
- Any $n$ packets should allow reconstruction of $n$ packet message.
- Any $n$ point values allow reconstruction of degree $n - 1$ polynomial.
Alright!!!
$n$ packet message, channel that loses $k$ packets.

Must send $n + k$ packets!

- Any $n$ packets should allow reconstruction of $n$ packet message.
- Any $n$ point values allow reconstruction of degree $n - 1$ polynomial.

Alright!!!!
Solution Idea.

\[ n \text{ packet message, channel that loses } k \text{ packets.} \]
Must send \( n + k \) packets!

- Any \textit{n packets} should allow reconstruction of \( n \) packet message.
- Any \textit{n point values} allow reconstruction of degree \( n - 1 \) polynomial.

Alright!!!!!
Solution Idea.

$n$ packet message, channel that loses $k$ packets.
Must send $n + k$ packets!

- Any $n$ packets should allow reconstruction of $n$ packet message.
- Any $n$ point values allow reconstruction of degree $n - 1$ polynomial.
Alright!!!!!!
Solution Idea.

$n$ packet message, channel that loses $k$ packets.
Must send $n + k$ packets!

Any $n$ packets should allow reconstruction of $n$ packet message.
Any $n$ point values allow reconstruction of degree $n - 1$ polynomial.
Alright!!!!!
Solution Idea.

\( n \) packet message, channel that loses \( k \) packets.
Must send \( n + k \) packets!

- Any \( n \) packets should allow reconstruction of \( n \) packet message.
- Any \( n \) point values allow reconstruction of degree \( n - 1 \) polynomial.

Alright!!!!!

Use polynomials.
Problem: Want to send a message with $n$ packets.
**Problem:** Want to send a message with \( n \) packets.

**Channel:** Lossy channel: loses \( k \) packets.
Problem: Want to send a message with $n$ packets.

Channel: Lossy channel: loses $k$ packets.

Question: Can you send $n+k$ packets and recover message?
Problem: Want to send a message with $n$ packets.
Channel: Lossy channel: loses $k$ packets.
Question: Can you send $n+k$ packets and recover message?
A degree $n-1$ polynomial determined by any $n$ points!
Problem: Want to send a message with \( n \) packets.

Channel: Lossy channel: loses \( k \) packets.

Question: Can you send \( n + k \) packets and recover message?

A degree \( n - 1 \) polynomial determined by any \( n \) points!

Erasure Coding Scheme: message = \( m_0, m_2, \ldots, m_{n-1} \).

1. Choose prime \( p \approx 2^b \) for packet size \( b \).
2. \( P(x) = m_{n-1}x^{n-1} + \cdots m_0 \) (mod \( p \)).
3. Send \( P(1), \ldots, P(n+k) \).
Problem: Want to send a message with $n$ packets.

Channel: Lossy channel: loses $k$ packets.

Question: Can you send $n+k$ packets and recover message?

A degree $n-1$ polynomial determined by any $n$ points!

Erasure Coding Scheme: message = $m_0, m_2, \ldots, m_{n-1}$.

1. Choose prime $p \approx 2^b$ for packet size $b$.
2. $P(x) = m_{n-1}x^{n-1} + \cdots m_0 \pmod{p}$.
3. Send $P(1), \ldots, P(n+k)$.

Any $n$ of the $n+k$ packets gives polynomial ...
Problem: Want to send a message with $n$ packets.
Channel: Lossy channel: loses $k$ packets.
Question: Can you send $n+k$ packets and recover message?
A degree $n-1$ polynomial determined by any $n$ points!
Erasure Coding Scheme: message = $m_0, m_2, \ldots, m_{n-1}$.

1. Choose prime $p \approx 2^b$ for packet size $b$.
2. $P(x) = m_{n-1}x^{n-1} + \cdots m_0 \pmod{p}$.
3. Send $P(1), \ldots, P(n+k)$.

Any $n$ of the $n+k$ packets gives polynomial ...and message!
Erasure Codes.

Satellite

GPS device
Erasure Codes.

Satellite

$n$ packet message.

GPS device

Any $n$ packets is enough!
Erasure Codes.

Satellite

GPS device

$n$ packet message.

Lose $k$ packets.
Erasure Codes.

Satellite

1 2 \cdots n+k

\text{Lose } k \text{ packets.}

GPS device

n \text{ packet message. So send } n+k!
Erasure Codes.

Satellite

1 2 ···· n+k

GPS device

$n$ packet message. So send $n+k$!

Lose $k$ packets.
Erasure Codes.

Satellite

\[ \begin{array}{cccccc}
1 & 2 & \cdots & n+k \\
\end{array} \]

GPS device

\[ \begin{array}{cccccc}
1 & 2 & \cdots & n+k \\
\end{array} \]

Lose \( k \) packets.

\( n \) packet message. So send \( n + k \)!

Optimal.
Erasure Codes.

Satellite

1 2 ⋮ \( n+k \)

GPS device

\( n \) packet message. So send \( n+k \)!

Lose \( k \) packets.

Any \( n \) packets is enough!
Erasure Codes.

Satellite

1 2 \ldots \ n+k

\[ \text{Lose } k \text{ packets.} \]

GPS device

1 2 \ldots \ n+k

Any \( n \) packets is enough!

\[ n \text{ packet message. So send } n+k! \]

\[ n \text{ packet message.} \]

Lose \( k \) packets.

Any \( n \) packets is enough!
Erasure Codes.

Satellite

1 2 \hspace{2cm} \cdots \hspace{2cm} n+k

\hspace{2cm} \cdots \\ 1 2 \hspace{2cm} \cdots \hspace{2cm} n+k

GPS device

Any $n$ packets is enough! $n$ packet message. So send $n+k$!

Lose $k$ packets.

Any $n$ packets is enough!

Optimal.
Information Theory.

Size: Can choose a prime between $2^{b-1}$ and $2^b$. (Lose at most 1 bit per packet.)
Size: Can choose a prime between $2^{b-1}$ and $2^b$. (Lose at most 1 bit per packet.)

But: packets need label for $x$ value.
Size: Can choose a prime between $2^{b-1}$ and $2^b$. (Lose at most 1 bit per packet.)
But: packets need label for $x$ value.
There are Galois Fields $GF(2^n)$ where one loses nothing.
Information Theory.

Size: Can choose a prime between $2^{b-1}$ and $2^b$.  
(Lose at most 1 bit per packet.)  
But: packets need label for $x$ value.  
There are Galois Fields $GF(2^n)$ where one loses nothing.  
– Can also run the Fast Fourier Transform.
Size: Can choose a prime between $2^{b-1}$ and $2^b$. (Lose at most 1 bit per packet.)

But: packets need label for $x$ value.

There are Galois Fields $GF(2^n)$ where one loses nothing.

– Can also run the Fast Fourier Transform.

In practice, $O(n)$ operations with almost the same redundancy.
Size: Can choose a prime between $2^{b-1}$ and $2^b$. (Lose at most 1 bit per packet.)

But: packets need label for $x$ value.

There are Galois Fields $GF(2^n)$ where one loses nothing.

– Can also run the Fast Fourier Transform.

In practice, $O(n)$ operations with almost the same redundancy.

Comparison with Secret Sharing: information content.
Size: Can choose a prime between $2^{b-1}$ and $2^b$. (Lose at most 1 bit per packet.)

But: packets need label for $x$ value.

There are Galois Fields $GF(2^n)$ where one loses nothing.

– Can also run the Fast Fourier Transform.

In practice, $O(n)$ operations with almost the same redundancy.

Comparison with Secret Sharing: information content.

  Secret Sharing: each share is size of whole secret.
Size: Can choose a prime between $2^{b-1}$ and $2^b$. (Lose at most 1 bit per packet.)

But: packets need label for $x$ value.

There are Galois Fields $GF(2^n)$ where one loses nothing.

– Can also run the Fast Fourier Transform.

In practice, $O(n)$ operations with almost the same redundancy.

Comparison with Secret Sharing: information content.

Secret Sharing: each share is size of whole secret.

Coding: Each packet has size $1/n$ of the whole message.
Information Theory.

Size: Can choose a prime between $2^{b-1}$ and $2^b$. (Lose at most 1 bit per packet.)
But: packets need label for $x$ value.
There are Galois Fields $GF(2^n)$ where one loses nothing.
– Can also run the Fast Fourier Transform.
In practice, $O(n)$ operations with almost the same redundancy.
Comparison with Secret Sharing: information content.
  Secret Sharing: each share is size of whole secret.
  Coding: Each packet has size $1/n$ of the whole message.
Erasure Code: Example.

Send message of 1, 4, and 4.

Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$.

How?

Lagrange Interpolation.
Linear System.
Work modulo 5.

$P(x) = x^2 \pmod{5}$

$P(1) = 1$, $P(2) = 4$, $P(3) = 9 = 4 \pmod{5}$

Send $(0, P(0)) ... (5, P(5))$.

6 points.

Better work modulo 7 at least!

Why?

$(0, P(0)) = (5, P(5)) \pmod{5}$
Erasure Code: Example.

Send message of 1,4, and 4.
Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$. 

Work modulo 5.

$$P(x) = x^2 \pmod{5}$$

$$P(1) = 1, P(2) = 4, P(3) = 4 \pmod{5}$$

Send $(0, P(0))$ ...

$(5, P(5))$. 6 points.

Better work modulo 7 at least!

Why?

$(0, P(0)) = (5, P(5)) \pmod{5}$
Erasure Code: Example.

Send message of 1, 4, and 4.
Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$.
How?
Erasure Code: Example.

Send message of 1, 4, and 4.
Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$.
How?
   Lagrange Interpolation.
Erasure Code: Example.

Send message of 1, 4, and 4.

Make polynomial with \( P(1) = 1, \ P(2) = 4, \ P(3) = 4. \)

How?

Lagrange Interpolation.
Linear System.
Erasure Code: Example.

Send message of 1, 4, and 4.

Make polynomial with \( P(1) = 1, P(2) = 4, P(3) = 4 \).

How?

Lagrange Interpolation.
Linear System.
Erasure Code: Example.

Send message of 1, 4, and 4.
Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$.
How?

- Lagrange Interpolation.
- Linear System.

Work modulo 5.
Send message of 1, 4, and 4.
Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$.

How?

Lagrange Interpolation.
Linear System.
Work modulo 5.

$P(x) = x^2 \pmod{5}$
Send message of 1, 4, and 4.
Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$.

How?

Lagrange Interpolation.
Linear System.

Work modulo 5.

$P(x) = x^2 \pmod{5}$

$P(1) = 1$, 

Better work modulo 7 at least!
Erasure Code: Example.

Send message of 1, 4, and 4.

Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$.

How?

Lagrange Interpolation.
Linear System.

Work modulo 5.

$$P(x) = x^2 \pmod{5}$$

$$P(1) = 1, P(2) = 4,$$
Send message of 1, 4, and 4.

Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$.

How?

Lagrange Interpolation.
Linear System.

Work modulo 5.

\[ P(x) = x^2 \pmod{5} \]

\[ P(1) = 1, \ P(2) = 4, \ P(3) = 9 = 4 \pmod{5} \]
Erasure Code: Example.

Send message of 1, 4, and 4.
Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$.

How?
Lagrange Interpolation.
Linear System.

Work modulo 5.

$P(x) = x^2 \pmod{5}$
$P(1) = 1$, $P(2) = 4$, $P(3) = 9 = 4 \pmod{5}$

Better work modulo 7 at least!
Erasure Code: Example.

Send message of 1, 4, and 4.

Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$.

How?

Lagrange Interpolation.
Linear System.

Work modulo 5.

$P(x) = x^2 \pmod{5}$

$P(1) = 1$, $P(2) = 4$, $P(3) = 9 = 4 \pmod{5}$

Send $(0, P(0)) \ldots (5, P(5))$. 
Erasure Code: Example.

Send message of 1, 4, and 4.

Make polynomial with \( P(1) = 1, \ P(2) = 4, \ P(3) = 4. \)

How?

Lagrange Interpolation.
Linear System.

Work modulo 5.

\[ P(x) = x^2 \pmod{5} \]

\[ P(1) = 1, \ P(2) = 4, \ P(3) = 9 = 4 \pmod{5} \]

Send \((0, P(0))\ldots(5, P(5))\).
Erasure Code: Example.

Send message of 1, 4, and 4.

Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$.

How?

Lagrange Interpolation.
Linear System.

Work modulo 5.

$P(x) = x^2 \pmod{5}$

$P(1) = 1$, $P(2) = 4$, $P(3) = 9 = 4 \pmod{5}$

Send $(0, P(0)) \ldots (5, P(5))$.

6 points.
Erasure Code: Example.

Send message of 1, 4, and 4.

Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$.

How?

Lagrange Interpolation.
Linear System.

Work modulo 5.

$$P(x) = x^2 \pmod{5}$$

$P(1) = 1$, $P(2) = 4$, $P(3) = 9 = 4 \pmod{5}$

Send $(0, P(0)) \ldots (5, P(5))$.

6 points. Better work modulo 7 at least!
Erasure Code: Example.

Send message of 1, 4, and 4.
Make polynomial with \( P(1) = 1, \ P(2) = 4, \ P(3) = 4 \).

How?

Lagrange Interpolation.
Linear System.

Work modulo 5.
\[ P(x) = x^2 \pmod{5} \]
\[ P(1) = 1, \ P(2) = 4, \ P(3) = 9 = 4 \pmod{5} \]

Send \((0, P(0)) \ldots (5, P(5))\).

6 points. Better work modulo 7 at least!

Why?
Erasure Code: Example.

Send message of 1, 4, and 4.

Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$.

How?

Lagrange Interpolation.
Linear System.

Work modulo 5.

$P(x) = x^2 \pmod{5}$

$P(1) = 1$, $P(2) = 4$, $P(3) = 9 = 4 \pmod{5}$

Send $(0, P(0)) \ldots (5, P(5))$.

6 points. Better work modulo 7 at least!

Why? $(0, P(0)) = (5, P(5)) \pmod{5}$
Example

Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$. 
Example

Make polynomial with \( P(1) = 1, P(2) = 4, P(3) = 4. \)
Modulo 7 to accommodate at least 6 packets.
Example

Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$. Modulo 7 to accommodate at least 6 packets.

Linear equations:
Example

Make polynomial with \( P(1) = 1, \ P(2) = 4, \ P(3) = 4. \)
Modulo 7 to accommodate at least 6 packets.
Linear equations:

\[
P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7}
\]

Send Packets: \((1, 1), (2, 4), (3, 4), (4, 7), (5, 2), (6, 0)\).
Notice that packets contain “x-values”.

Example

Make polynomial with \( P(1) = 1, \ P(2) = 4, \ P(3) = 4. \)
Modulo 7 to accommodate at least 6 packets.
Linear equations:

\[
P(1) = a_2 + a_1 + a_0 \quad \equiv \quad 1 \pmod{7}
\]
\[
P(2) = 4a_2 + 2a_1 + a_0 \quad \equiv \quad 4 \pmod{7}
\]
Example

Make polynomial with \( P(1) = 1, \ P(2) = 4, \ P(3) = 4. \)
Modulo 7 to accommodate at least 6 packets.
Linear equations:

\[
P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7}\\P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7}\\P(3) = 2a_2 + 3a_1 + a_0 \equiv 4 \pmod{7}
\]
Example

Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$.
Modulo 7 to accommodate at least 6 packets.
Linear equations:

$$P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7}$$
$$P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7}$$
$$P(3) = 2a_2 + 3a_1 + a_0 \equiv 4 \pmod{7}$$
Example

Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$. Modulo 7 to accommodate at least 6 packets.

Linear equations:

\begin{align*}
    P(1) &= a_2 + a_1 + a_0 \equiv 1 \pmod{7} \\
    P(2) &= 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7} \\
    P(3) &= 2a_2 + 3a_1 + a_0 \equiv 4 \pmod{7}
\end{align*}

$6a_1 + 3a_0 = 2 \pmod{7}$,
Example

Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$. Modulo 7 to accommodate at least 6 packets.

Linear equations:

\begin{align*}
P(1) &= a_2 + a_1 + a_0 \equiv 1 \pmod{7} \\
P(2) &= 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7} \\
P(3) &= 2a_2 + 3a_1 + a_0 \equiv 4 \pmod{7} \\
6a_1 + 3a_0 &= 2 \pmod{7}, \quad 5a_1 + 4a_0 = 0 \pmod{7}
\end{align*}
Example

Make polynomial with \( P(1) = 1, \ P(2) = 4, \ P(3) = 4. \)
Modulo 7 to accommodate at least 6 packets.
Linear equations:

\[
\begin{align*}
P(1) &= a_2 + a_1 + a_0 \equiv 1 \pmod{7} \\
P(2) &= 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7} \\
P(3) &= 2a_2 + 3a_1 + a_0 \equiv 4 \pmod{7}
\end{align*}
\]

\[6a_1 + 3a_0 = 2 \pmod{7}, \quad 5a_1 + 4a_0 = 0 \pmod{7}\]
\[a_1 = 2a_0.\]
Example

Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$.
Modulo 7 to accommodate at least 6 packets.
Linear equations:

\[
P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7}
\]
\[
P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7}
\]
\[
P(3) = 2a_2 + 3a_1 + a_0 \equiv 4 \pmod{7}
\]

\[
6a_1 + 3a_0 = 2 \pmod{7}, \quad 5a_1 + 4a_0 = 0 \pmod{7}
\]

\[
a_1 = 2a_0, \quad a_0 = 2 \pmod{7}
\]
Example

Make polynomial with \( P(1) = 1, \ P(2) = 4, \ P(3) = 4. \)
Modulo 7 to accommodate at least 6 packets.
Linear equations:

\[
P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7} \\
P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7} \\
P(3) = 2a_2 + 3a_1 + a_0 \equiv 4 \pmod{7}
\]

\[6a_1 + 3a_0 = 2 \pmod{7}, \ 5a_1 + 4a_0 = 0 \pmod{7}\]

\[a_1 = 2a_0, \ a_0 = 2 \pmod{7}, \ a_1 = 4 \pmod{7}\]
Example

Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$.
Modulo 7 to accommodate at least 6 packets.
Linear equations:

$P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7}$
$P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7}$
$P(3) = 2a_2 + 3a_1 + a_0 \equiv 4 \pmod{7}$

$6a_1 + 3a_0 = 2 \pmod{7}$, $5a_1 + 4a_0 = 0 \pmod{7}$

$a_1 = 2a_0$, $a_0 = 2 \pmod{7}$, $a_1 = 4 \pmod{7}$, $a_2 = 2 \pmod{7}$
Example

Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$.
Modulo 7 to accommodate at least 6 packets.
Linear equations:

$P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7}$
$P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7}$
$P(3) = 2a_2 + 3a_1 + a_0 \equiv 4 \pmod{7}$

$6a_1 + 3a_0 = 2 \pmod{7}$, $5a_1 + 4a_0 = 0 \pmod{7}$
$a_1 = 2a_0$, $a_0 = 2 \pmod{7}$ $a_1 = 4 \pmod{7}$ $a_2 = 2 \pmod{7}$

$P(x) = 2x^2 + 4x + 2$
Example

Make polynomial with $P(1) = 1, \ P(2) = 4, \ P(3) = 4$.
Modulo 7 to accommodate at least 6 packets.
Linear equations:

\[
\begin{align*}
P(1) &= a_2 + a_1 + a_0 \equiv 1 \pmod{7} \\
P(2) &= 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7} \\
P(3) &= 2a_2 + 3a_1 + a_0 \equiv 4 \pmod{7}
\end{align*}
\]

\[6a_1 + 3a_0 = 2 \pmod{7}, \quad 5a_1 + 4a_0 = 0 \pmod{7}\]

\[a_1 = 2a_0, \quad a_0 = 2 \pmod{7}, \quad a_1 = 4 \pmod{7}, \quad a_2 = 2 \pmod{7}\]

$P(x) = 2x^2 + 4x + 2$
Example

Make polynomial with \( P(1) = 1 \), \( P(2) = 4 \), \( P(3) = 4 \).
Modulo 7 to accommodate at least 6 packets.
Linear equations:

\[
P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7} \\
P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7} \\
P(3) = 2a_2 + 3a_1 + a_0 \equiv 4 \pmod{7}
\]

\[
6a_1 + 3a_0 = 2 \pmod{7}, \quad 5a_1 + 4a_0 = 0 \pmod{7}
\]

\[
a_1 = 2a_0, \quad a_0 = 2 \pmod{7} \quad a_1 = 4 \pmod{7} \quad a_2 = 2 \pmod{7}
\]

\[
P(x) = 2x^2 + 4x + 2
\]

\[
P(1) = 1,
\]
Make polynomial with \( P(1) = 1, P(2) = 4, P(3) = 4 \).
Modulo 7 to accommodate at least 6 packets.
Linear equations:

\[
\begin{align*}
P(1) &= a_2 + a_1 + a_0 \equiv 1 \pmod{7} \\
P(2) &= 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7} \\
P(3) &= 2a_2 + 3a_1 + a_0 \equiv 4 \pmod{7}
\end{align*}
\]

\[
6a_1 + 3a_0 = 2 \pmod{7}, \quad 5a_1 + 4a_0 = 0 \pmod{7}
\]

\[
a_1 = 2a_0, \quad a_0 = 2 \pmod{7}, \quad a_1 = 4 \pmod{7}, \quad a_2 = 2 \pmod{7}
\]

\[
P(x) = 2x^2 + 4x + 2
\]

\[
P(1) = 1, \quad P(2) = 4,
\]
Example

Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$. Modulo 7 to accommodate at least 6 packets.

Linear equations:

$$P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7}$$
$$P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7}$$
$$P(3) = 2a_2 + 3a_1 + a_0 \equiv 4 \pmod{7}$$

$$6a_1 + 3a_0 = 2 \pmod{7}, \quad 5a_1 + 4a_0 = 0 \pmod{7}$$

$$a_1 = 2a_0, \quad a_0 = 2 \pmod{7}, \quad a_1 = 4 \pmod{7}, \quad a_2 = 2 \pmod{7}$$

$$P(x) = 2x^2 + 4x + 2$$

$P(1) = 1$, $P(2) = 4$, and $P(3) = 4$
Example

Make polynomial with \( P(1) = 1, P(2) = 4, P(3) = 4 \).
Modulo 7 to accommodate at least 6 packets.

Linear equations:

\[
\begin{align*}
P(1) &= a_2 + a_1 + a_0 \equiv 1 \pmod{7} \\
P(2) &= 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7} \\
P(3) &= 2a_2 + 3a_1 + a_0 \equiv 4 \pmod{7}
\end{align*}
\]

\[
6a_1 + 3a_0 = 2 \pmod{7}, \quad 5a_1 + 4a_0 = 0 \pmod{7}
\]

\[
a_1 = 2a_0, \quad a_0 = 2 \pmod{7}, \quad a_1 = 4 \pmod{7}, \quad a_2 = 2 \pmod{7}
\]

\[
P(x) = 2x^2 + 4x + 2
\]

\[
P(1) = 1, \ P(2) = 4, \ \text{and} \ P(3) = 4
\]
Example

Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$.
Modulo 7 to accommodate at least 6 packets.

Linear equations:

\[
P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7}
\]
\[
P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7}
\]
\[
P(3) = 2a_2 + 3a_1 + a_0 \equiv 4 \pmod{7}
\]

\[
6a_1 + 3a_0 = 2 \pmod{7}, \quad 5a_1 + 4a_0 = 0 \pmod{7}
\]

\[
a_1 = 2a_0, \quad a_0 = 2 \pmod{7}, \quad a_1 = 4 \pmod{7}, \quad a_2 = 2 \pmod{7}
\]

\[
P(x) = 2x^2 + 4x + 2
\]

$P(1) = 1$, $P(2) = 4$, and $P(3) = 4$

Send
Example

Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$.
Modulo 7 to accommodate at least 6 packets.

Linear equations:

\[
P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7} \\
P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7} \\
P(3) = 2a_2 + 3a_1 + a_0 \equiv 4 \pmod{7}
\]

\[
6a_1 + 3a_0 = 2 \pmod{7}, \quad 5a_1 + 4a_0 = 0 \pmod{7}
\]

\[
a_1 = 2a_0, \quad a_0 = 2 \pmod{7} \quad a_1 = 4 \pmod{7} \quad a_2 = 2 \pmod{7}
\]

\[
P(x) = 2x^2 + 4x + 2
\]

\[
P(1) = 1, \quad P(2) = 4, \quad \text{and} \quad P(3) = 4
\]

Send

Packets: (1, 1), (2, 4), (3, 4), (4, 7), (5, 2), (6, 0)
Example

Make polynomial with $P(1) = 1$, $P(2) = 4$, $P(3) = 4$.
Modulo 7 to accommodate at least 6 packets.
Linear equations:

$P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7}$
$P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7}$
$P(3) = 2a_2 + 3a_1 + a_0 \equiv 4 \pmod{7}$

$6a_1 + 3a_0 = 2 \pmod{7}, \ 5a_1 + 4a_0 = 0 \pmod{7}$

$a_1 = 2a_0. \ a_0 = 2 \pmod{7} \ a_1 = 4 \pmod{7} \ a_2 = 2 \pmod{7}$

$P(x) = 2x^2 + 4x + 2$

$P(1) = 1, P(2) = 4, \text{ and } P(3) = 4$

Send
Packets: $(1, 1), (2, 4), (3, 4), (4, 7), (5, 2), (6, 0)$

Notice that packets contain “x-values”.

Bad reception!

Send: (1, 1), (2, 4), (3, 4), (4, 7), (5, 2), (6, 0)
Bad reception!

Send: (1, 1), (2, 4), (3, 4), (4, 7), (5, 2), (6, 0)
Recieve: (1, 1) (3, 4), (6, 0)
Bad reception!

Send: (1, 1), (2, 4), (3, 4), (4, 7), (5, 2), (6, 0)

Receive: (1, 1) (3, 4), (6, 0)

Reconstruct?
Bad reception!

Send: (1, 1), (2, 4), (3, 4), (4, 7), (5, 2), (6, 0)
Recieve: (1, 1) (3, 4), (6, 0)
   Reconstruct?
Format: (i, R(i)).
Bad reception!

Send: (1,1), (2,4), (3,4), (4,7), (5,2), (6,0)

Recieve: (1,1) (3,4), (6,0)
    Reconstruct?

Format: $(i, R(i))$.

Lagrange or linear equations.
Bad reception!

Send: \((1,1), (2,4), (3,4), (4,7), (5,2), (6,0)\)

Receive: \((1,1), (3,4), (6,0)\)

Reconstruct?

Format: \((i, R(i))\).

Lagrange or linear equations.

\[
P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7}
\]
Bad reception!

Send: (1, 1), (2, 4), (3, 4), (4, 7), (5, 2), (6, 0)

Recieve: (1, 1) (3, 4), (6, 0)
Reconstruct?

Format: (i, R(i)).

Lagrange or linear equations.

\[ P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7} \]
\[ P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7} \]
Bad reception!

Send: (1, 1), (2, 4), (3, 4), (4, 7), (5, 2), (6, 0)

Receive: (1, 1), (3, 4), (6, 0)

Reconstruct?

Format: \((i, R(i))\).

Lagrange or linear equations.

\[
P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7}
\]
\[
P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7}
\]
\[
P(6) = 2a_2 + 3a_1 + a_0 \equiv 0 \pmod{7}
\]
Bad reception!

Send: (1, 1), (2, 4), (3, 4), (4, 7), (5, 2), (6, 0)

Receive: (1, 1) (3, 4), (6, 0)
Reconstruct?

Format: \((i, R(i))\).

Lagrange or linear equations.

\[
P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7}
\]
\[
P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7}
\]
\[
P(6) = 2a_2 + 3a_1 + a_0 \equiv 0 \pmod{7}
\]
Bad reception!

Send: (1,1), (2,4), (3,4), (4,7), (5,2), (6,0)

Receive: (1,1) (3,4), (6,0)
Reconstruct?

Format: (i, R(i)).
Lagrange or linear equations.

\[ P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7} \]
\[ P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7} \]
\[ P(6) = 2a_2 + 3a_1 + a_0 \equiv 0 \pmod{7} \]

Channeling Sahai
Bad reception!

Send: \((1, 1), (2, 4), (3, 4), (4, 7), (5, 2), (6, 0)\)

Recieve: \((1, 1), (3, 4), (6, 0)\)

Reconstruct?

Format: \((i, R(i))\).

Lagrange or linear equations.

\[
P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7}
\]
\[
P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7}
\]
\[
P(6) = 2a_2 + 3a_1 + a_0 \equiv 0 \pmod{7}
\]

Channeling Sahai ...

Bad reception!

Send: \( (1, 1), (2, 4), (3, 4), (4, 7), (5, 2), (6, 0) \)

Receive: \( (1, 1), (3, 4), (6, 0) \)

Reconstruct?

Format: \( (i, R(i)) \).

Lagrange or linear equations.

\[
P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7}
\]

\[
P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7}
\]

\[
P(6) = 2a_2 + 3a_1 + a_0 \equiv 0 \pmod{7}
\]

Channeling Sahai ...

\[
P(x) = 2x^2 + 4x + 2
\]
Bad reception!

Send: (1, 1), (2, 4), (3, 4), (4, 7), (5, 2), (6, 0)

Recieve: (1, 1) (3, 4), (6, 0)
Reconstruct?

Format: \((i, R(i))\).

Lagrange or linear equations.

\[
P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7}
\]
\[
P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7}
\]
\[
P(6) = 2a_2 + 3a_1 + a_0 \equiv 0 \pmod{7}
\]

Channeling Sahai ...

\[
P(x) = 2x^2 + 4x + 2
\]
Bad reception!

Send: $(1, 1), (2, 4), (3, 4), (4, 7), (5, 2), (6, 0)$

Recieve: $(1, 1), (3, 4), (6, 0)$
   
Reconstruct?

Format: $(i, R(i))$.

Lagrange or linear equations.

\[
P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7} \\
P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7} \\
P(6) = 2a_2 + 3a_1 + a_0 \equiv 0 \pmod{7}
\]

Channeling Sahai ...

\[
P(x) = 2x^2 + 4x + 2
\]

Message?
Bad reception!

Send: (1, 1), (2, 4), (3, 4), (4, 7), (5, 2), (6, 0)

Recieve: (1,1) (3,4), (6,0)
Reconstruct?

Format: (i, R(i)).

Lagrange or linear equations.

\[
P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7} \\
P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7} \\
P(6) = 2a_2 + 3a_1 + a_0 \equiv 0 \pmod{7}
\]

Channeling Sahai ... 
\[P(x) = 2x^2 + 4x + 2\]

Message? \( P(1) = 1, \)
Bad reception!

Send: \((1, 1), (2, 4), (3, 4), (4, 7), (5, 2), (6, 0)\)

Recieve: \((1, 1), (3, 4), (6, 0)\)

Reconstruct?

Format: \((i, R(i))\).

Lagrange or linear equations.

\[
P(1) = a_2 + a_1 + a_0 \equiv 1 \pmod{7}
\]

\[
P(2) = 4a_2 + 2a_1 + a_0 \equiv 4 \pmod{7}
\]

\[
P(6) = 2a_2 + 3a_1 + a_0 \equiv 0 \pmod{7}
\]

Channeling Sahai ...

\[
P(x) = 2x^2 + 4x + 2
\]

Message? \(P(1) = 1, P(2) = 4,\)
Bad reception!

Send: (1, 1), (2, 4), (3, 4), (4, 7), (5, 2), (6, 0)

Recieve: (1,1) (3,4), (6,0)
Reconstruct?

Format: \((i, R(i))\).
Lagrange or linear equations.

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

Channeling Sahai ...

\[ P(x) = 2x^2 + 4x + 2 \]
Message? \( P(1) = 1, P(2) = 4, P(3) = 4. \)
You want to encode a secret consisting of 1,4,4.
You want to encode a secret consisting of 1,4,4.

How big should modulus be?
You want to encode a secret consisting of 1,4,4.

How big should modulus be?
Larger than 144
Questions for Review

You want to encode a secret consisting of 1,4,4.

How big should modulus be?
Larger than 144 and prime!
Questions for Review

You want to encode a secret consisting of 1,4,4.

How big should modulus be?
Larger than 144 and prime!

You want to send a message consisting of packets 1,4,2,3,0

Send $n$ packets $b$-bit packets, with $k$ errors.
Modulus should be larger than $n + k$ and also larger than $2^b$. 
You want to encode a secret consisting of 1, 4, 4.

How big should modulus be?
Larger than 144 and prime!

You want to send a message consisting of packets 1, 4, 2, 3, 0 through a noisy channel that loses 3 packets.
Questions for Review

You want to encode a secret consisting of 1,4,4.
   How big should modulus be?
   Larger than 144 and prime!

You want to send a message consisting of packets 1,4,2,3,0
   through a noisy channel that loses 3 packets.
   How big should modulus be?
Questions for Review

You want to encode a secret consisting of 1, 4, 4.

How big should modulus be?
Larger than 144 and prime!

You want to send a message consisting of packets 1, 4, 2, 3, 0 through a noisy channel that loses 3 packets.
How big should modulus be?
Questions for Review

You want to encode a secret consisting of 1,4,4.
   How big should modulus be?
   Larger than 144 and prime!

You want to send a message consisting of packets 1,4,2,3,0 through a noisy channel that loses 3 packets.
   How big should modulus be?
   Larger than 8
Questions for Review

You want to encode a secret consisting of 1, 4, 4.

How big should modulus be?
Larger than 144 and prime!

You want to send a message consisting of packets 1, 4, 2, 3, 0 through a noisy channel that loses 3 packets.

How big should modulus be?
Larger than 8 and prime!
Questions for Review

You want to encode a secret consisting of 1,4,4. How big should modulus be? Larger than 144 and prime!

You want to send a message consisting of packets 1,4,2,3,0 through a noisy channel that loses 3 packets. How big should modulus be? Larger than 8 and prime!

Send $n$ packets $b$-bit packets, with $k$ errors.
Questions for Review

You want to encode a secret consisting of 1, 4, 4.

How big should modulus be?
Larger than 144 and prime!

You want to send a message consisting of packets 1, 4, 2, 3, 0 through a noisy channel that loses 3 packets.

How big should modulus be?
Larger than 8 and prime!

Send $n$ packets $b$-bit packets, with $k$ errors.
Modulus should be larger than $n + k$ and also larger than $2^b$. 
Polynomials.
Polynomials.

- give Secret Sharing.

Error Correction: Noisy Channel: corrupts $k$ packets. (rather than loss.) Additional Challenge: Finding which packets are corrupt.
Polynomials.

- give Secret Sharing.
- give Erasure Codes.
Polynomials.

- give Secret Sharing.
- give Erasure Codes.

Error Correction:
Polynomials.

- give Secret Sharing.
- give Erasure Codes.

**Error Correction:**

Noisy Channel: corrupts $k$ packets. (rather than loss.)
Polynomials.

- give Secret Sharing.
- give Erasure Codes.

**Error Correction:**

Noisy Channel: corrupts $k$ packets. (rather than loss.)

Additional Challenge: Finding which packets are corrupt.
Error Correction

Satellite

GPS device
Error Correction

Satellite

GPS device

3 packet message.
Error Correction

Satellite

3 packet message.

GPS device

Corrupts 1 packets.
Error Correction

Satellite

1 2 3 1 2
A B C D E

3 packet message. Send 5.

Corrupts 1 packets.

GPS device
Error Correction

Satellite

3 packet message. Send 5.

Corrupts 1 packets.
Error Correction

3 packet message. Send 5.

Corrupts 1 packets.
At least...

To correct $k$ errors need $2k$ extra packets.
At least...

To correct $k$ errors need $2k$ extra packets.

$\text{Encoding}(m) = p_1, p_2, \ldots, p_n, \ldots p_{n+2k-1}$.
At least...

To correct $k$ errors need $2k$ extra packets.

Encoding$(m) = p_1, p_2, \ldots, p_n, \ldots p_{n+2k-1}$.

Encoding$(m') = p_1, p_2, \ldots, p'_n, \ldots p'_{n+2k-1}$.
At least...

To correct $k$ errors need $2k$ extra packets.

$\text{Encoding}(m) = p_1, p_2, \ldots, p_n, \ldots p_{n+2k-1}.$

$\text{Encoding}(m') = p_1, p_2, \ldots, p'_n, \ldots p'_{n+2k-1}.$
At least...

To correct $k$ errors need $2k$ extra packets.

Encoding($m$) = $p_1, p_2, \ldots, p_n, \ldots p_{n+2k-1}$.

Encoding($m'$) = $p_1, p_2, \ldots, p'_n, \ldots p'_{n+2k-1}$.

$k$ changes from either can make following message
At least...

To correct $k$ errors need $2k$ extra packets.

Encoding($m$) = $p_1, p_2, \ldots, p_n, \ldots, p_{n+2k-1}$.
Encoding($m'$) = $p_1, p_2, \ldots, p'_n, \ldots, p'_{n+2k-1}$.

$k$ changes from either can make following message

$p_1, p_2, \ldots, p_n, \ldots, p_{n+k-1}, p'_{n+k} \ldots, p'_{n+2k-1}$
At least...

To correct $k$ errors need $2k$ extra packets.

Encoding($m$) = $p_1, p_2, \ldots, p_n, \ldots, p_{n+2k-1}$.

Encoding($m'$)= $p_1, p_2, \ldots, p'_n, \ldots, p'_{n+2k-1}$.

$k$ changes from either can make following message

$$p_1, p_2, \ldots, p_n, \ldots, p_{n+k-1}, p'_{n+k}, \ldots, p'_{n+2k-1}$$

Which message did received word come from???
At least...

To correct $k$ errors need $2k$ extra packets.

Encoding($m$) = $p_1, p_2, \ldots, p_n, \ldots p_{n+2k-1}$.

Encoding($m'$) = $p_1, p_2, \ldots, p'_n, \ldots p'_{n+2k-1}$.

$k$ changes from either can make following message

$p_1, p_2, \ldots, p_n, \ldots, p_{n+k-1}, p'_{n+k}, \ldots, p'_{n+2k-1}$

Which message did received word come from???

Can’t tell which message is which with $k$ errors!
At least...

To correct $k$ errors need $2k$ extra packets.

$\text{Encoding}(m) = p_1, p_2, \ldots, p_n, \ldots p_{n+2k-1}$

$\text{Encoding}(m') = p_1, p_2, \ldots, p'_n, \ldots p'_{n+2k-1}$

$k$ changes from either can make following message

\[p_1, p_2, \ldots, p_n, \ldots, p_{n+k-1}, p'_{n+k}, \ldots, p'_{n+2k-1}\]

Which message did received word come from???

Can’t tell which message is which with $k$ errors!

\textbf{Information theory intuition:}
To correct $k$ errors need $2k$ extra packets.

Encoding($m$) = $p_1, p_2, \ldots, p_n, \ldots p_{n+2k-1}$.

Encoding($m'$) = $p_1, p_2, \ldots, p'_n, \ldots p'_{n+2k-1}$.

$k$ changes from either can make following message

$p_1, p_2, \ldots, p_n, \ldots, p_{n+k-1}, p'_{n+k} \ldots, p'_{n+2k-1}$

Which message did received word come from???

Can’t tell which message is which with $k$ errors!

**Information theory intuition:**

$m$ packets sent
At least...

To correct $k$ errors need $2k$ extra packets.

Encoding($m$) = $p_1, p_2, \ldots, p_n, \ldots p_{n+2k-1}$.

Encoding($m'$)= $p_1, p_2, \ldots, p'_n, \ldots p'_{n+2k-1}$.

$k$ changes from either can make following message

$$p_1, p_2, \ldots, p_n, \ldots, p_{n+k-1}, p'_{n+k} \ldots, p'_{n+2k-1}$$

Which message did received word come from???

Can’t tell which message is which with $k$ errors!

**Information theory intuition:**

$m$ packets sent

$n$ units of information need to be transmitted.
At least...

To correct $k$ errors need $2k$ extra packets.

$\text{Encoding}(m) = p_1, p_2, \ldots, p_n, \ldots p_{n+2k-1}$.

$\text{Encoding}(m') = p_1, p_2, \ldots, p'n, \ldots p'_{n+2k-1}$.

$k$ changes from either can make following message

$p_1, p_2, \ldots, p_n, \ldots, p_{n+k-1}, p'_{n+k}, \ldots, p'_{n+2k-1}$

Which message did received word come from???

Can’t tell which message is which with $k$ errors!

**Information theory intuition:**

$m$ packets sent
$n$ units of information need to be transmitted.
$k$ units of information/packets destroyed by channel.
At least...

To correct $k$ errors need $2k$ extra packets.

Encoding($m$) = $p_1, p_2, \ldots, p_n, \ldots p_{n+2k-1}$.

Encoding($m'$) = $p_1, p_2, \ldots, p'_n, \ldots p'_{n+2k-1}$.

$k$ changes from either can make following message

$p_1, p_2, \ldots, p_n, \ldots, p_{n+k-1}, p'_{n+k} \ldots, p'_{n+2k-1}$

Which message did received word come from???

Can’t tell which message is which with $k$ errors!

**Information theory intuition:**

$m$ packets sent

$n$ units of information need to be transmitted.

$k$ units of information/packets destroyed by channel.

$k$ units of information added by channel!!!!!!
At least...

To correct $k$ errors need $2k$ extra packets.

Encoding($m$) = $p_1, p_2, \ldots, p_n, \ldots p_{n+2k-1}$.

Encoding($m'$) = $p_1, p_2, \ldots, p'_n, \ldots p'_{n+2k-1}$.

$k$ changes from either can make following message

$p_1, p_2, \ldots, p_n, \ldots, p_{n+k-1}, p'_{n+k} \ldots, p'_{n+2k-1}$

Which message did recieved word come from???

Can’t tell which message is which with $k$ errors!

**Information theory intuition:**

$m$ packets sent

$n$ units of information need to be transmitted.

$k$ units of information/packets destroyed by channel.

$k$ units of information added by channel!!!!!

which $k$ packets are destroyed.
At least...

To correct $k$ errors need $2k$ extra packets.

Encoding($m$) = $p_1, p_2, \ldots, p_n, \ldots, p_{n+2k-1}$.

Encoding($m'$) = $p_1, p_2, \ldots, p'_n, \ldots, p'_{n+2k-1}$.

$k$ changes from either can make following message

\[ p_1, p_2, \ldots, p_n, \ldots, p_{n+k-1}, p'_{n+k} \ldots, p'_{n+2k-1} \]

Which message did received word come from???

Can’t tell which message is which with $k$ errors!

**Information theory intuition:**

$m$ packets sent

$n$ units of information need to be transmitted.

$k$ units of information/packets destroyed by channel.

$k$ units of information added by channel!!!!!!

which $k$ packets are destroyed.

Better have $m - k$
At least...

To correct $k$ errors need $2k$ extra packets.

Encoding($m$) = $p_1, p_2, \ldots, p_n, \ldots p_{n+2k-1}$.

Encoding($m'$) = $p_1, p_2, \ldots, p'_n, \ldots p'_{n+2k-1}$.

$k$ changes from either can make following message

$p_1, p_2, \ldots, p_n, \ldots, p_{n+k-1}, p'_{n+k} \ldots, p'_{n+2k-1}$

Which message did received word come from???

Can’t tell which message is which with $k$ errors!

Information theory intuition:

$m$ packets sent

$n$ units of information need to be transmitted.

$k$ units of information/packets destroyed by channel.

$k$ units of information added by channel!!!!!!

which $k$ packets are destroyed.

Better have $m - k \geq n + k$. 
At least...

To correct $k$ errors need $2k$ extra packets.

Encoding($m$) = $p_1, p_2, \ldots, p_n, \ldots p_{n+2k-1}$.

Encoding($m'$) = $p_1, p_2, \ldots, p'_n, \ldots p'_{n+2k-1}$.

$k$ changes from either can make following message

$p_1, p_2, \ldots, p_n, \ldots, p_{n+k-1}, p'_{n+k} \ldots, p'_{n+2k-1}$

Which message did recieved word come from???

Can’t tell which message is which with $k$ errors!

Information theory intuition:

$m$ packets sent

$n$ units of information need to be transmitted.

$k$ units of information/packets destroyed by channel.

$k$ units of information added by channel!!!!!!

which $k$ packets are destroyed.

Better have $m - k \geq n + k. \implies m \geq n + 2k$. 
The Scheme.

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

**Reed-Solomon Code:**
The Scheme.

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.
   - $P(1) = m_1, \ldots, P(n) = m_n$.
The Scheme.

**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.
   - $P(1) = m_1, \ldots, P(n) = m_n$.
   - Comment: could encode with packets as coefficients.
The Scheme.

**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.
   - \(P(1) = m_1, \ldots, P(n) = m_n\).
   - Comment: could encode with packets as coefficients.

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

**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.
   - $P(1) = m_1, \ldots, P(n) = m_n$.
   - Comment: could encode with packets as coefficients.

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

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

**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.
   - \( P(1) = m_1, \ldots, P(n) = m_n. \)
   - Comment: could encode with packets as coefficients.

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 \( i \),
The Scheme.

**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.
   - $P(1) = m_1, \ldots, P(n) = m_n$.
   - Comment: could encode with packets as coefficients.
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
The Scheme.

**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.
   - $P(1) = m_1, \ldots, P(n) = m_n$.
   - Comment: could encode with packets as coefficients.

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

**After noisy channel:** Recive 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.
Properties: proof.

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

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

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

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

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

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

**Properties:**

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

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

Properties:
(1) \(P(i) = R(i)\) for at least \(n + k\) points \(i\),
(2) \(P(x)\) is unique degree \(n - 1\) polynomial
Properties: proof.

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

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.
Properties: proof.

$P(x)$: degree $n - 1$ polynomial.

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

Receive $R(1),...,R(n+2k)$

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

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.
Properties: proof.

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

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

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

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

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.

Proof:
Properties: proof.

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

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

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

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

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.

Proof: (1) Sure.
Properties: proof.

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

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.

Proof: (1) Sure. Only \( k \) corruptions.
Properties: proof.

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

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.

Proof: (1) Sure. Only \( k \) corruptions.
(2) Degree \( n - 1 \) polynomial \( Q(x) \) consistent with \( n + k \) points.
Properties: proof.

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

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.

Proof: (1) Sure. Only \( k \) corruptions.
(2) Degree \( n - 1 \) polynomial \( Q(x) \) consistent with \( n + k \) points.
\( Q(x) \) and \( P(x) \) agrees with \( R(i), n + k \) times.
Properties: proof.

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

**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.

**Proof:** (1) Sure. Only \(k\) corruptions.
(2) Degree \(n - 1\) polynomial \(Q(x)\) consistent with \(n + k\) points.
    \(Q(x)\) and \(P(x)\) agrees with \(R(i)\), \(n + k\) times.
    Total agreements with \(R(i)\) : \(2n + 2k\).
Properties: proof.

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

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.

Proof: (1) Sure. Only \( k \) corruptions.
(2) Degree \( n - 1 \) polynomial \( Q(x) \) consistent with \( n + k \) points.
\( Q(x) \) and \( P(x) \) agrees with \( R(i) \), \( n + k \) times.
    Total agreements with \( R(i) \) : \( 2n + 2k \). \( P \) Pigeons.
Properties: proof.

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

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.

Proof: (1) Sure. Only \( k \) corruptions.
(2) Degree \( n - 1 \) polynomial \( Q(x) \) consistent with \( n + k \) points.
\( Q(x) \) and \( P(x) \) agrees with \( R(i) \), \( n + k \) times.
    Total agreements with \( R(i) \) : \( 2n + 2k \).
    Pigeons.
Total points to agree : \( n + 2k \).
Properties: proof.

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

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.

Proof: (1) Sure. Only \( k \) corruptions.
(2) Degree \( n - 1 \) polynomial \( Q(x) \) consistent with \( n+k \) points.
    \( Q(x) \) and \( P(x) \) agrees with \( R(i) \), \( n+k \) times.
    Total agreements with \( R(i) \) : \( 2n+2k \).
    Total points to agree : \( n+2k \).
    Pigeons. Holes.
Properties: proof.

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

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.

Proof:  (1) Sure. Only \( k \) corruptions.
(2) Degree \( n - 1 \) polynomial \( Q(x) \) consistent with \( n + k \) points.
    \( Q(x) \) and \( P(x) \) agrees with \( R(i) \), \( n + k \) times.
    Total agreements with \( R(i) \) : \( 2n + 2k \).
    Total points to agree : \( n + 2k \).
    Collisions : \( \geq n \).
Properties: proof.

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

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.

Proof: (1) Sure. Only \( k \) corruptions.
(2) Degree \( n - 1 \) polynomial \( Q(x) \) consistent with \( n + k \) points.
\( Q(x) \) and \( P(x) \) agrees with \( R(i), n + k \) times.
Total agreements with \( R(i) \) : \( 2n + 2k \). \( P \) Pigeons.
Total points to agree : \( n + 2k \). \( H \) Holes.
Collisions : \( \geq n \). \( \geq P - H \) Collisions.
Properties: proof.

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

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.

Proof: (1) Sure. Only \( k \) corruptions.
(2) Degree \( n - 1 \) polynomial \( Q(x) \) consistent with \( n + k \) points.
\( Q(x) \) and \( P(x) \) agrees with \( R(i) \), \( n + k \) times.
   Total agreements with \( R(i) \): \( 2n + 2k \). \( P \) Pigeons.
   Total points to agree: \( n + 2k \). \( H \) Holes.
   Collisions: \( \geq n \). \( \geq P - H \) Collisions.
   Agreements per point: \( 2 \).
Properties: proof.

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

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.

Proof: (1) Sure. Only \( k \) corruptions.
(2) Degree \( n - 1 \) polynomial \( Q(x) \) consistent with \( n + k \) points.
    \( Q(x) \) and \( P(x) \) agrees with \( R(i) \), \( n + k \) times.
    Total agreements with \( R(i) \) : \( 2n + 2k \).
    Total points to agree : \( n + 2k \).
    Collisions : \( \geq n \).
    Agreements per point : \( 2 \).
    \( P - H \) Collisions.
Properties: proof.

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

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.

Proof: (1) Sure. Only \( k \) corruptions.
(2) Degree \( n - 1 \) polynomial \( Q(x) \) consistent with \( n+k \) points.
\( Q(x) \) and \( P(x) \) agrees with \( R(i) \), \( n+k \) times.

Total agreements with \( R(i) \): \( 2n+2k \). \( P \) Pigeons.
Total points to agree: \( n+2k \). \( H \) Holes.
Collisions: \( \geq n \). \( \geq P - H \) Collisions.
Agreements per point: \( 2 \). 1 collision per hole.
Points \( Q(x) \) and \( P(x) \) agree: \( \geq n \).
Properties: proof.

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

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.

Proof: (1) Sure. Only \( k \) corruptions.
(2) Degree \( n - 1 \) polynomial \( Q(x) \) consistent with \( n + k \) points.

\( Q(x) \) and \( P(x) \) agrees with \( R(i), n + k \) times.
Total agreements with \( R(i) \) : \( 2n + 2k \). \( P \) Pigeons.
Total points to agree : \( n + 2k \). \( H \) Holes.
Collisions : \( \geq n \). \( \geq P - H \) Collisions.
Agreements per point : 2. 1 collision per hole.
Points \( Q(x) \) and \( P(x) \) agree : \( \geq n \). \( \geq P - H \) holes w/collision.
\( \implies \) \( Q(i) = P(i) \) at \( n \) points.
Properties: proof.

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

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.

Proof: (1) Sure. Only \( k \) corruptions.
(2) Degree \( n-1 \) polynomial \( Q(x) \) consistent with \( n+k \) points.
\( Q(x) \) and \( P(x) \) agrees with \( R(i) \), \( n+k \) times.
Total agreements with \( R(i) \) : \( 2n+2k \). \( P \) \begin{align*}
\text{Pigeons.}
\end{align*}
Total points to agree : \( n+2k \). \( H \) \begin{align*}
\text{Holes.}
\end{align*}
Collisions : \( \geq n \). \( \geq P-H \) Collisions.
Agreements per point : \( 2 \). \begin{align*}
1 \text{ collision per hole.}
\end{align*}
Points \( Q(x) \) and \( P(x) \) agree : \( \geq n \). \begin{align*}
\geq P-H \text{ holes w/collision.}
\end{align*}
\( \implies Q(i) = P(i) \) at \( n \) points. \( \implies Q(x) = P(x) \).
Properties: proof.

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

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.

Proof: (1) Sure. Only \( k \) corruptions.
(2) Degree \( n - 1 \) polynomial \( Q(x) \) consistent with \( n + k \) points.

\( Q(x) \) and \( P(x) \) agrees with \( R(i), n + k \) times.
Total agreements with \( R(i) \) : \( 2n + 2k \).
Total points to agree : \( n + 2k \).
Collisions : \( \geq n \).
Agreements per point : 2.
Points \( Q(x) \) and \( P(x) \) agree : \( \geq n \).
\( \implies Q(i) = P(i) \) at \( n \) points. \( \implies Q(x) = P(x) \).
Example.

Message: 3, 0, 6.
Example.

Message: 3, 0, 6.

Reed Solomon Code: $P(x) = x^2 + x + 1 \pmod{7}$ has $P(1) = 3, P(2) = 0, P(3) = 6 \pmod{7}$. 
Example.

Message: 3, 0, 6.

Reed Solomon Code: $P(x) = x^2 + x + 1 \pmod{7}$ has $P(1) = 3, P(2) = 0, P(3) = 6 \pmod{7}$.

Send: $P(1) = 3, P(2) = 0, P(3) = 6,$
Example.

Message: 3, 0, 6.
Reed Solomon Code: $P(x) = x^2 + x + 1 \pmod{7}$ has
$P(1) = 3, P(2) = 0, P(3) = 6$ modulo 7.
Send: $P(1) = 3, P(2) = 0, P(3) = 6, P(4) = 0, P(5) = 3.$
Example.

Message: 3, 0, 6.

Reed Solomon Code: $P(x) = x^2 + x + 1 \pmod{7}$ has $P(1) = 3, P(2) = 0, P(3) = 6$ modulo 7.

Send: $P(1) = 3, P(2) = 0, P(3) = 6, P(4) = 0, P(5) = 3$.

(Aside: Message in plain text!)
Example.

Message: 3, 0, 6.
Reed Solomon Code: $P(x) = x^2 + x + 1 \pmod{7}$ has $P(1) = 3, P(2) = 0, P(3) = 6$ modulo 7.
Send: $P(1) = 3, P(2) = 0, P(3) = 6, P(4) = 0, P(5) = 3$.
(Aside: Message in plain text!)
Receive $R(1) = 3, R(2) = 1, R(3) = 6, R(4) = 0, R(5) = 3$. 
Example.

Message: 3, 0, 6.

Reed Solomon Code: \( P(x) = x^2 + x + 1 \) (mod 7) has
\( P(1) = 3, P(2) = 0, P(3) = 6 \) modulo 7.

Send: \( P(1) = 3, P(2) = 0, P(3) = 6, P(4) = 0, P(5) = 3 \).

(Aside: Message in plain text!)

Receive \( R(1) = 3, R(2) = 1, R(3) = 6, R(4) = 0, R(5) = 3 \).

\( P(i) = R(i) \) for \( n + k = 3 + 1 = 4 \) points.
Slow solution.

Brute Force:
For each subset of $n + k$ points
Slow solution.

**Brute Force:**
For each subset of $n + k$ points
  - Fit degree $n - 1$ polynomial, $Q(x)$, to $n$ of them.
Slow solution.

**Brute Force:**
For each subset of \( n + k \) points
- Fit degree \( n - 1 \) polynomial, \( Q(x) \), to \( n \) of them.
- Check if consistent with \( n + k \) of the total points.
Slow solution.

**Brute Force:**
For each subset of \( n + k \) points
- Fit degree \( n - 1 \) polynomial, \( Q(x) \), to \( n \) of them.
- Check if consistent with \( n + k \) of the total points.
- If yes, output \( Q(x) \).
Slow solution.

**Brute Force:**
For each subset of $n+k$ points
  Fit degree $n-1$ polynomial, $Q(x)$, to $n$ of them.
  Check if consistent with $n+k$ of the total points.
  If yes, output $Q(x)$.

- For subset of $n+k$ pts where $R(i) = P(i)$,
  method will reconstruct $P(x)$!
Slow solution.

**Brute Force:**
For each subset of $n + k$ points
  Fit degree $n - 1$ polynomial, $Q(x)$, to $n$ of them.
  Check if consistent with $n + k$ of the total points.
  If yes, output $Q(x)$.

- For subset of $n + k$ pts where $R(i) = P(i)$,
  method will reconstruct $P(x)$!
- For any subset of $n + k$ pts,
Slow solution.

**Brute Force:**
For each subset of $n+k$ points
   Fit degree $n-1$ polynomial, $Q(x)$, to $n$ of them.
   Check if consistent with $n+k$ of the total points.
   If yes, output $Q(x)$.

- For subset of $n+k$ pts where $R(i) = P(i)$, method will reconstruct $P(x)$!
- For any subset of $n+k$ pts,
  1. there is unique degree $n-1$ polynomial $Q(x)$ that fits $n$ of them
Slow solution.

**Brute Force:**
For each subset of $n+k$ points
   Fit degree $n-1$ polynomial, $Q(x)$, to $n$ of them.
   Check if consistent with $n+k$ of the total points.
   If yes, output $Q(x)$.

- For subset of $n+k$ pts where $R(i) = P(i)$,
  method will reconstruct $P(x)$!

- For any subset of $n+k$ pts,
  1. there is unique degree $n-1$ polynomial $Q(x)$ that fits $n$ of them
  2. and where $Q(x)$ is consistent with $n+k$ points
Slow solution.

**Brute Force:**
For each subset of $n + k$ points
- Fit degree $n - 1$ polynomial, $Q(x)$, to $n$ of them.
- Check if consistent with $n + k$ of the total points.
  If yes, output $Q(x)$.

- For subset of $n + k$ pts where $R(i) = P(i)$, method will reconstruct $P(x)$!
- For any subset of $n + k$ pts,
  1. there is unique degree $n - 1$ polynomial $Q(x)$ that fits $n$ of them
  2. and where $Q(x)$ is consistent with $n + k$ points
     \[\Rightarrow P(x) = Q(x).\]
Slow solution.

**Brute Force:**
For each subset of $n + k$ points
  Fit degree $n - 1$ polynomial, $Q(x)$, to $n$ of them.
  Check if consistent with $n + k$ of the total points.
  If yes, output $Q(x)$.

- For subset of $n + k$ pts where $R(i) = P(i)$,
  method will reconstruct $P(x)$!

- For any subset of $n + k$ pts,
  1. there is unique degree $n - 1$ polynomial $Q(x)$ that fits $n$ of them
  2. and where $Q(x)$ is consistent with $n + k$ points
     $\Rightarrow P(x) = Q(x)$.

Reconstructs $P(x)$ and only $P(x)$!!
Example.

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

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

Find $P(x) = p_2 x^2 + p_1 x + p_0$ that contains $n + k = 3 + 1$ points.
Example.

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

Find $P(x) = p_2x^2 + p_1x + p_0$ that contains $n + k = 3 + 1$ points.

All equations:

\[
\begin{align*}
p_2 + p_1 + p_0 & \equiv 3 \pmod{7} \\
4p_2 + 2p_1 + p_0 & \equiv 1 \pmod{7} \\
2p_2 + 3p_1 + p_0 & \equiv 6 \pmod{7} \\
2p_2 + 4p_1 + p_0 & \equiv 0 \pmod{7} \\
1p_2 + 5p_1 + p_0 & \equiv 3 \pmod{7}
\end{align*}
\]
Example.

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

Find $P(x) = p_2x^2 + p_1x + p_0$ that contains $n + k = 3 + 1$ points.

All equations:

\[
\begin{align*}
   p_2 + p_1 + p_0 & \equiv 3 \pmod{7} \\
   4p_2 + 2p_1 + p_0 & \equiv 1 \pmod{7} \\
   2p_2 + 3p_1 + p_0 & \equiv 6 \pmod{7} \\
   2p_2 + 4p_1 + p_0 & \equiv 0 \pmod{7} \\
   1p_2 + 5p_1 + p_0 & \equiv 3 \pmod{7}
\end{align*}
\]

Assume point 1 is wrong

Assume point 2 is wrong... consistent solution!
Example.

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

Find $P(x) = p_2 x^2 + p_1 x + p_0$ that contains $n + k = 3 + 1$ points.

All equations.

\[
\begin{align*}
    p_2 + p_1 + p_0 & \equiv 3 \pmod{7} \\
    4p_2 + 2p_1 + p_0 & \equiv 1 \pmod{7} \\
    2p_2 + 3p_1 + p_0 & \equiv 6 \pmod{7} \\
    2p_2 + 4p_1 + p_0 & \equiv 0 \pmod{7} \\
    1p_2 + 5p_1 + p_0 & \equiv 3 \pmod{7}
\end{align*}
\]

Assume point 1 is wrong and solve..
Example.

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

Find \( P(x) = p_2 x^2 + p_1 x + p_0 \) that contains \( n + k = 3 + 1 \) points.

All equations..

\[
\begin{align*}
   p_2 + p_1 + p_0 & \equiv 3 \pmod{7} \\
   4p_2 + 2p_1 + p_0 & \equiv 1 \pmod{7} \\
   2p_2 + 3p_1 + p_0 & \equiv 6 \pmod{7} \\
   2p_2 + 4p_1 + p_0 & \equiv 0 \pmod{7} \\
   1p_2 + 5p_1 + p_0 & \equiv 3 \pmod{7}
\end{align*}
\]

Assume point 1 is wrong and solve.. no consistent solution!
Example.

Received $R(1) = 3, R(2) = 1, R(3) = 6, R(4) = 0, R(5) = 3$
Find $P(x) = p_2 x^2 + p_1 x + p_0$ that contains $n + k = 3 + 1$ points.
All equations..

\[
\begin{align*}
    p_2 + p_1 + p_0 & \equiv 3 \pmod{7} \\
    4p_2 + 2p_1 + p_0 & \equiv 1 \pmod{7} \\
    2p_2 + 3p_1 + p_0 & \equiv 6 \pmod{7} \\
    2p_2 + 4p_1 + p_0 & \equiv 0 \pmod{7} \\
    1p_2 + 5p_1 + p_0 & \equiv 3 \pmod{7}
\end{align*}
\]

Assume point 1 is wrong and solve.. no consistent solution!
Assume point 2 is wrong
Example.

Received $R(1) = 3, R(2) = 1, R(3) = 6, R(4) = 0, R(5) = 3$
Find $P(x) = p_2 x^2 + p_1 x + p_0$ that contains $n + k = 3 + 1$ points.

All equations..

$$p_2 + p_1 + p_0 \equiv 3 \pmod{7}$$
$$4p_2 + 2p_1 + p_0 \equiv 1 \pmod{7}$$
$$2p_2 + 3p_1 + p_0 \equiv 6 \pmod{7}$$
$$2p_2 + 4p_1 + p_0 \equiv 0 \pmod{7}$$
$$1p_2 + 5p_1 + p_0 \equiv 3 \pmod{7}$$

Assume point 1 is wrong and solve..no consistent solution!
Assume point 2 is wrong and solve...
Example.

Received $R(1) = 3, R(2) = 1, R(3) = 6, R(4) = 0, R(5) = 3$
Find $P(x) = p_2 x^2 + p_1 x + p_0$ that contains $n + k = 3 + 1$ points.
All equations..

\[
\begin{align*}
p_2 + p_1 + p_0 & \equiv 3 \pmod{7} \\
4p_2 + 2p_1 + p_0 & \equiv 1 \pmod{7} \\
2p_2 + 3p_1 + p_0 & \equiv 6 \pmod{7} \\
2p_2 + 4p_1 + p_0 & \equiv 0 \pmod{7} \\
1p_2 + 5p_1 + p_0 & \equiv 3 \pmod{7}
\end{align*}
\]

Assume point 1 is wrong and solve.. \textit{no consistent solution}!
Assume point 2 is wrong and solve... \textit{consistent solution}!
In general,

\[ P(x) = p_{n-1}x^{n-1} + \cdots + p_0 \]

and receive \( R(1), \ldots R(m = n + 2k) \).
In general,

\[ P(x) = p_{n-1}x^{n-1} + \cdots + p_0 \] and receive \( R(1), \ldots, R(m = n+2k) \).

\[ p_{n-1} + \cdots + p_0 \equiv R(1) \pmod{p} \]
In general..

\[ P(x) = p_{n-1}x^{n-1} + \cdots p_0 \]

and receive \( R(1), \ldots R(m = n + 2k) \).

\[
\begin{align*}
p_{n-1} + \cdots p_0 & \equiv R(1) \pmod{p} \\
p_{n-1}2^{n-1} + \cdots p_0 & \equiv R(2) \pmod{p}
\end{align*}
\]
In general,

\[ P(x) = p_{n-1}x^{n-1} + \cdots + p_0 \] and receive \( R(1), \ldots, R(m = n + 2k) \).

\[ p_{n-1} + \cdots + p_0 \equiv R(1) \pmod{p} \]
\[ p_{n-1}2^{n-1} + \cdots + p_0 \equiv R(2) \pmod{p} \]
\[ \vdots \]
\[ p_{n-1}i^{n-1} + \cdots + p_0 \equiv R(i) \pmod{p} \]
\[ \vdots \]
\[ p_{n-1}(m)^{n-1} + \cdots + p_0 \equiv R(m) \pmod{p} \]
In general,

\[ P(x) = p_{n-1}x^{n-1} + \cdots + p_0 \] and receive \( R(1), \ldots, R(m = n + 2k) \).

\[
\begin{align*}
p_{n-1} + \cdots + p_0 & \equiv R(1) \pmod{p} \\
p_{n-1}2^{n-1} + \cdots + p_0 & \equiv R(2) \pmod{p} \\
& \quad \vdots \\
p_{n-1}i^{n-1} + \cdots + p_0 & \equiv R(i) \pmod{p} \\
& \quad \vdots \\
p_{n-1}(m)^{n-1} + \cdots + p_0 & \equiv R(m) \pmod{p}
\end{align*}
\]

Error!!
In general, 

\[ P(x) = p_{n-1}x^{n-1} + \cdots + p_0 \] and receive \( R(1), \ldots, R(m = n + 2k) \).

\[
\begin{align*}
p_{n-1} + \cdots + p_0 & \equiv R(1) \pmod{p} \\
p_{n-1}2^{n-1} + \cdots + p_0 & \equiv R(2) \pmod{p} \\
& \vdots \\
p_{n-1}i^{n-1} + \cdots + p_0 & \equiv R(i) \pmod{p} \\
& \vdots \\
p_{n-1}(m)^{n-1} + \cdots + p_0 & \equiv R(m) \pmod{p}
\end{align*}
\]

Error!! .... Where???
In general,

\[ P(x) = p_{n-1}x^{n-1} + \cdots + p_0 \] and receive \( R(1), \ldots, R(m = n + 2k) \).

\begin{align*}
p_{n-1} + \cdots + p_0 & \equiv R(1) \pmod{p} \\
p_{n-1}2^{n-1} + \cdots + p_0 & \equiv R(2) \pmod{p} \\
\quad & \quad \quad \vdots \\
p_{n-1}i^{n-1} + \cdots + p_0 & \equiv R(i) \pmod{p} \\
\quad & \quad \quad \vdots \\
p_{n-1}(m)^{n-1} + \cdots + p_0 & \equiv R(m) \pmod{p}
\end{align*}

Error!! .... Where???
Could be anywhere!!!
In general,

\[ P(x) = p_{n-1}x^{n-1} + \cdots p_0 \] and receive \( R(1), \ldots, R(m = n + 2k) \).

\[
\begin{align*}
p_{n-1} + \cdots + p_0 & \equiv R(1) \pmod{p} \\
p_{n-1}2^{n-1} + \cdots + p_0 & \equiv R(2) \pmod{p} \\
& \quad \vdots \\
p_{n-1}i^{n-1} + \cdots + p_0 & \equiv R(i) \pmod{p} \\
& \quad \vdots \\
p_{n-1}(m)^{n-1} + \cdots + p_0 & \equiv R(m) \pmod{p}
\end{align*}
\]

Error!! .... Where???
Could be anywhere!!! ...so try everywhere.
In general,

\[ P(x) = p_{n-1}x^{n-1} + \cdots + p_0 \] and receive \( R(1), \ldots, R(m = n + 2k) \).

\[
\begin{align*}
p_{n-1} + \cdots + p_0 & \equiv R(1) \pmod{p} \\
p_{n-1}2^{n-1} + \cdots + p_0 & \equiv R(2) \pmod{p} \\
\vdots & \\
p_{n-1}i^{n-1} + \cdots + p_0 & \equiv R(i) \pmod{p} \\
\vdots & \\
p_{n-1}(m)^{n-1} + \cdots + p_0 & \equiv R(m) \pmod{p}
\end{align*}
\]

Error!! .... Where???
Could be anywhere!!! ...so try everywhere.

**Runtime:** \( \binom{n+2k}{k} \) possibilities.
In general,

\[ P(x) = p_{n-1}x^{n-1} + \cdots + p_0 \] and receive \( R(1), \ldots, R(m = n+2k) \).

\[
\begin{align*}
p_{n-1} + \cdots + p_0 & \equiv R(1) \pmod{p} \\
p_{n-1}2^{n-1} + \cdots + p_0 & \equiv R(2) \pmod{p} \\
\vdots & \\
p_{n-1}i^{n-1} + \cdots + p_0 & \equiv R(i) \pmod{p} \\
\vdots & \\
p_{n-1}(m)^{n-1} + \cdots + p_0 & \equiv R(m) \pmod{p}
\end{align*}
\]

Error!! .... Where???
Could be anywhere!!! ...so try everywhere.

**Runtime:** \( \binom{n+2k}{k} \) possibilities.

Something like \( (n/k)^k \) ...Exponential in \( k \)!
In general..

\[ P(x) = p_{n-1}x^{n-1} + \cdots p_0 \] and receive \( R(1), \ldots R(m = n + 2k). \)

\[
\begin{align*}
p_{n-1} + \cdots p_0 & \equiv R(1) \pmod{p} \\
p_{n-1}2^{n-1} + \cdots p_0 & \equiv R(2) \pmod{p} \\
& \quad \vdots \\
p_{n-1}i^{n-1} + \cdots p_0 & \equiv R(i) \pmod{p} \\
& \quad \vdots \\
p_{n-1}(m)^{n-1} + \cdots p_0 & \equiv R(m) \pmod{p}
\end{align*}
\]

Error!! .... Where???
Could be anywhere!!! ...so try everywhere.

**Runtime:** \( \binom{n+2k}{k} \) possibilities.

Something like \( (n/k)^k \) ...Exponential in \( k \!).

How do we find where the bad packets are efficiently?!?!?!
Ditty...

Oh where, Oh where

Oh where, Oh where
Oh where, Oh where has my little dog gone?

Oh where, oh where can he be
With his ears cut short
And his tail cut long
Oh where, oh where can he be?

Where oh where have my little packets gone... bad.
Ditty...

Oh where, Oh where
has my little dog gone?
Oh where, oh where can he be
Oh where, Oh where
has my little dog gone?
Oh where, oh where can he be

With his ears cut short
Oh where, Oh where
has my little dog gone?
Oh where, oh where can he be

With his ears cut short
And his tail cut long
Oh where, Oh where
has my little dog gone?
Oh where, oh where can he be

With his ears cut short
And his tail cut long
Oh where, oh where can he be?
Oh where, Oh where
has my little dog gone?
Oh where, oh where can he be
With his ears cut short
And his tail cut long
Oh where, oh where can he be?

Where oh where have my little packets gone ...
Ditty...

Oh where, Oh where
has my little dog gone?
Oh where, oh where can he be

With his ears cut short
And his tail cut long
Oh where, oh where can he be?

Where oh where have my little packets gone ...bad.
Where oh where can my **bad packets** be?

\[(p_{n−1} + ⋯ p_0) \equiv R(1) \pmod{p}\]
Where oh where can my **bad packets** be?

\[
(p_{n-1} + \cdots p_0) \equiv R(1) \quad \text{(mod } p) \\
(p_{n-1}2^{n-1} + \cdots p_0) \equiv R(2) \quad \text{(mod } p) \\
\vdots \\
(p_{n-1}(m)^{n-1} + \cdots p_0) \equiv R(n+2k) \quad \text{(mod } p)
\]
Where oh where can my bad packets be?

\[
\begin{align*}
(p_{n-1} + \cdots + p_0) & \equiv R(1) \pmod{p} \\
(p_{n-1}2^{n-1} + \cdots + p_0) & \equiv R(2) \pmod{p} \\
& \quad \vdots \\
(p_{n-1}(m)^{n-1} + \cdots + p_0) & \equiv R(n+2k) \pmod{p}
\end{align*}
\]

**Idea:** Multiply equation \( i \) by 0 if and only if \( P(i) \neq R(i) \).
Where oh where can my bad packets be?

$$
(p_{n-1} + \cdots + p_0) \equiv R(1) \pmod{p} \\
0 \times (p_{n-1}2^{n-1} + \cdots + p_0) \equiv R(2) \pmod{p} \\
\vdots \\
(p_{n-1}(m)^{n-1} + \cdots + p_0) \equiv R(n+2k) \pmod{p}
$$

Idea: Multiply equation $i$ by 0 if and only if $P(i) \neq R(i)$. All equations satisfied!!!!!
Where oh where can my bad packets be?

\[(p_{n-1} + \cdots p_0) \equiv R(1) \pmod{p}\]
\[(p_{n-1}2^{n-1} + \cdots p_0) \equiv R(2) \pmod{p}\]
\[
\vdots 
\]
\[(p_{n-1}(m)^{n-1} + \cdots p_0) \equiv R(n+2k) \pmod{p}\]

Idea: Multiply equation \(i\) by 0 if and only if \(P(i) \neq R(i)\).
All equations satisfied!!!!!

But which equations should we multiply by 0?
Where oh where can my **bad packets** be?

\[(p_{n-1} + \cdots + p_0) \equiv R(1) \pmod{p}\]
\[(p_{n-1}2^{n-1} + \cdots + p_0) \equiv R(2) \pmod{p}\]
\[\vdots\]
\[(p_{n-1}(m)^{n-1} + \cdots + p_0) \equiv R(n+2k) \pmod{p}\]

**Idea:** Multiply equation \(i\) by 0 if and only if \(P(i) \neq R(i)\).
All equations satisfied!!!!!

But which equations should we multiply by 0? *Where oh where...*
Where oh where can my bad packets be?

\[
(p_{n-1} + \cdots + p_0) \equiv R(1) \pmod{p} \\
(p_{n-1}2^{n-1} + \cdots + p_0) \equiv R(2) \pmod{p} \\
\vdots \\
(p_{n-1}(m)^{n-1} + \cdots + p_0) \equiv R(n+2k) \pmod{p}
\]

**Idea:** Multiply equation \( i \) by 0 if and only if \( P(i) \neq R(i) \). All equations satisfied!!!!!

But which equations should we multiply by 0? Where oh where...??
Where oh where can my bad packets be?

\[(p_{n-1} + \cdots + p_0) \equiv R(1) \pmod{p}\]
\[(p_{n-1}2^{n-1} + \cdots + p_0) \equiv R(2) \pmod{p}\]
\[\vdots\]
\[(p_{n-1}(m)^{n-1} + \cdots + p_0) \equiv R(n+2k) \pmod{p}\]

**Idea:** Multiply equation \(i\) by 0 if and only if \(P(i) \neq R(i)\). All equations satisfied!!!!

But which equations should we multiply by 0? Where oh where...??

We will use a polynomial!!!
Where oh where can my **bad packets** be?

\[
(p_{n-1} + \cdots + p_0) \equiv R(1) \pmod{p}
\]
\[
(p_{n-1}2^{n-1} + \cdots + p_0) \equiv R(2) \pmod{p}
\]
\[\vdots\]
\[
(p_{n-1}(m)^{n-1} + \cdots + p_0) \equiv R(n + 2k) \pmod{p}
\]

**Idea:** Multiply equation \(i\) by 0 if and only if \(P(i) \neq R(i)\).

All equations satisfied!!!!!!

But which equations should we multiply by 0? Where oh where...??

We will use a polynomial!!! That we don’t know.
Where oh where can my bad packets be?

\[
(p_{n-1} + \cdots + p_0) \equiv R(1) \pmod{p}
\]
\[
(p_{n-1}2^{n-1} + \cdots + p_0) \equiv R(2) \pmod{p}
\]
\[
\vdots
\]
\[
(p_{n-1}(m)^{n-1} + \cdots + p_0) \equiv R(n+2k) \pmod{p}
\]

Idea: Multiply equation \(i\) by 0 if and only if \(P(i) \neq R(i)\). All equations satisfied!!!!!

But which equations should we multiply by 0? Where oh where...??

We will use a polynomial!!! That we don’t know. But can find!
Where oh where can my **bad packets** be?

\[(p_{n-1} + \cdots + p_0) \equiv R(1) \pmod{p}\]
\[(p_{n-1}2^{n-1} + \cdots + p_0) \equiv R(2) \pmod{p}\]
\[\vdots\]
\[(p_{n-1}(m)^{n-1} + \cdots + p_0) \equiv R(n+2k) \pmod{p}\]

**Idea:** Multiply equation \(i\) by 0 if and only if \(P(i) \neq R(i)\).
All equations satisfied!!!!!

But which equations should we multiply by 0? **Where oh where...??**

We will use a polynomial!!! That we don’t know. But can find!

Errors at points \(e_1, \ldots, e_k\). (In diagram above, \(e_1 = 2\).)
Where oh where can my **bad packets** be?

\[
(p_{n-1} + \cdots + p_0) \equiv R(1) \pmod{p}
\]

\[
(p_{n-1}2^{n-1} + \cdots + p_0) \equiv R(2) \pmod{p}
\]

\[\vdots\]

\[
(p_{n-1}(m)^{n-1} + \cdots + p_0) \equiv R(n+2k) \pmod{p}
\]

**Idea:** Multiply equation \(i\) by 0 if and only if \(P(i) \neq R(i)\).

All equations satisfied!!!!!

But which equations should we multiply by 0? Where oh where...??

**We will use a polynomial!!!** That we don't know. But can find!

Errors at points \(e_1, \ldots, e_k\). (In diagram above, \(e_1 = 2\).)

**Error locator polynomial:** \(E(x) = (x - e_1)\)
Where oh where can my bad packets be?

\[
(p_{n-1} + \cdots + p_0) \equiv R(1) \pmod{p} \\
(p_{n-1}2^{n-1} + \cdots + p_0) \equiv R(2) \pmod{p} \\
\vdots \\
(p_{n-1}(m)^{n-1} + \cdots + p_0) \equiv R(n+2k) \pmod{p}
\]

Idea: Multiply equation \( i \) by 0 if and only if \( P(i) \neq R(i) \).
All equations satisfied!!!!!

But which equations should we multiply by 0? Where oh where...??

We will use a polynomial!!! That we don’t know. But can find!

Errors at points \( e_1, \ldots, e_k \). (In diagram above, \( e_1 = 2 \).)

Error locator polynomial: \( E(x) = (x - e_1)(x - e_2) \)
Where oh where can my **bad packets** be?

\[
(p_{n-1} + \cdots p_0) \equiv R(1) \pmod{p} \\
(p_{n-1}2^{n-1} + \cdots p_0) \equiv R(2) \pmod{p} \\
\vdots \\
(p_{n-1}(m)^{n-1} + \cdots p_0) \equiv R(n+2k) \pmod{p}
\]

**Idea:** Multiply equation \(i\) by 0 if and only if \(P(i) \neq R(i)\).
All equations satisfied!!!!!

But which equations should we multiply by 0? **Where oh where...??**

**We will use a polynomial!!!** That we don’t know. But can find!

Errors at points \(e_1, \ldots, e_k\). (In diagram above, \(e_1 = 2\).)

**Error locator polynomial:** \(E(x) = (x - e_1)(x - e_2)\ldots\)
Where oh where can my **bad packets** be?

\[
(p_{n-1} + \cdots p_0) \equiv R(1) \pmod{p}
\]
\[
(p_{n-1}2^{n-1} + \cdots p_0) \equiv R(2) \pmod{p}
\]
\[
\vdots
\]
\[
(p_{n-1}(m)^{n-1} + \cdots p_0) \equiv R(n+2k) \pmod{p}
\]

**Idea:** Multiply equation \( i \) by 0 if and only if \( P(i) \neq R(i) \).

All equations satisfied!!!!!

But which equations should we multiply by 0? Where oh where...??

We will use a polynomial!!! That we don’t know. But can find!

Errors at points \( e_1, \ldots, e_k \). (In diagram above, \( e_1 = 2 \).)

**Error locator polynomial:** \( E(x) = (x - e_1)(x - e_2) \ldots (x - e_k) \).
Where oh where can my bad packets be?

\[(p_{n-1} + \cdots + p_0) \equiv R(1) \pmod{p}\]
\[(p_{n-1}2^{n-1} + \cdots + p_0) \equiv R(2) \pmod{p}\]
\[\vdots\]
\[(p_{n-1}(m)^{n-1} + \cdots + p_0) \equiv R(n+2k) \pmod{p}\]

Idea: Multiply equation \(i\) by 0 if and only if \(P(i) \neq R(i)\).
All equations satisfied!!!!!

But which equations should we multiply by 0? Where oh where...??

We will use a polynomial!!! That we don’t know. But can find!

Errors at points \(e_1, \ldots, e_k\). (In diagram above, \(e_1 = 2\).)

**Error locator polynomial:** \(E(x) = (x - e_1)(x - e_2)\ldots(x - e_k)\).

\(E(i) = 0\) if and only if \(e_j = i\) for some \(j\)
Where oh where can my bad packets be?

\[
E(1)(p_{n-1} + \cdots p_0) \equiv R(1)E(1) \pmod{p} \\
E(2)(p_{n-1}2^{n-1} + \cdots p_0) \equiv R(2)E(2) \pmod{p} \\
\vdots \\
E(m)(p_{n-1}(m)^{n-1} + \cdots p_0) \equiv R(n+2k)E(m) \pmod{p}
\]

Idea: Multiply equation \( i \) by 0 if and only if \( P(i) \neq R(i) \).
All equations satisfied!!!!!!

But which equations should we multiply by 0? Where oh where...??

We will use a polynomial!!! That we don’t know. But can find!

Errors at points \( e_1, \ldots, e_k \). (In diagram above, \( e_1 = 2 \).)

**Error locator polynomial**: \( E(x) = (x - e_1)(x - e_2)\cdots(x - e_k) \).

\( E(i) = 0 \) if and only if \( e_j = i \) for some \( j \)

Multiply equations by \( E(\cdot) \).
Where oh where can my **bad packets** be?

\[
E(1)(\rho_{n-1} + \cdots \rho_0) \equiv R(1)E(1) \pmod{p}
\]
\[
E(2)(\rho_{n-1}2^{n-1} + \cdots \rho_0) \equiv R(2)E(2) \pmod{p}
\]
\[
\vdots
\]
\[
E(m)(\rho_{n-1}(m)^{n-1} + \cdots \rho_0) \equiv R(n+2k)E(m) \pmod{p}
\]

**Idea:** Multiply equation \(i\) by 0 if and only if \(P(i) \neq R(i)\).
All equations satisfied!!!!!!

But which equations should we multiply by 0? Where oh where...??

**We will use a polynomial!!!** That we don’t know. But can find!

Errors at points \(e_1, \ldots, e_k\). (In diagram above, \(e_1 = 2\).)

**Error locator polynomial:** \(E(x) = (x - e_1)(x - e_2) \cdots (x - e_k)\).

\(E(i) = 0\) if and only if \(e_j = i\) for some \(j\)

Multiply equations by \(E(\cdot)\). (Above \(E(x) = (x-2)\).)
Where oh where can my bad packets be?

\[
E(1)(\rho_{n-1} + \cdots + \rho_0) \equiv R(1)E(1) \pmod p \\
E(2)(\rho_{n-1}2^{n-1} + \cdots + \rho_0) \equiv R(2)E(2) \pmod p \\
\vdots \\
E(m)(\rho_{n-1}(m)^{n-1} + \cdots + \rho_0) \equiv R(n+2k)E(m) \pmod p
\]

**Idea:** Multiply equation \(i\) by 0 if and only if \(P(i) \neq R(i)\).

All equations satisfied!!!!!

But which equations should we multiply by 0? Where oh where...??

We will use a polynomial!!! That we don’t know. But can find!

Errors at points \(e_1, \ldots, e_k\). (In diagram above, \(e_1 = 2\).)

**Error locator polynomial:** \(E(x) = (x-e_1)(x-e_2)\ldots(x-e_k)\).

\(E(i) = 0\) if and only if \(e_j = i\) for some \(j\)

Multiply equations by \(E(\cdot)\). (Above \(E(x) = (x-2)\).)

All equations satisfied!!
Example.

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

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

Find $P(x) = p_2 x^2 + p_1 x + p_0$ that contains $n + k = 3 + 1$ points.
Example.

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

Find $P(x) = p_2 x^2 + p_1 x + p_0$ that contains $n + k = 3 + 1$ points.

Plugin points...

\[
\begin{align*}
(p_2 + p_1 + p_0) & \equiv (3) \pmod{7} \\
(4p_2 + 2p_1 + p_0) & \equiv (1) \pmod{7} \\
(2p_2 + 3p_1 + p_0) & \equiv (6) \pmod{7} \\
(2p_2 + 4p_1 + p_0) & \equiv (0) \pmod{7} \\
(4p_2 + 5p_1 + p_0) & \equiv (3) \pmod{7}
\end{align*}
\]
Example.

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

Find $P(x) = p_2 x^2 + p_1 x + p_0$ that contains $n + k = 3 + 1$ points.

Plugin points...

\[
\begin{align*}
(p_2 + p_1 + p_0) & \equiv (3) \quad \text{(mod 7)} \\
(4p_2 + 2p_1 + p_0) & \equiv (1) \quad \text{(mod 7)} \\
(2p_2 + 3p_1 + p_0) & \equiv (6) \quad \text{(mod 7)} \\
(2p_2 + 4p_1 + p_0) & \equiv (0) \quad \text{(mod 7)} \\
(4p_2 + 5p_1 + p_0) & \equiv (3) \quad \text{(mod 7)}
\end{align*}
\]

Error locator polynomial: $(x - 2)$. 
Example.

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

Find $P(x) = p_2 x^2 + p_1 x + p_0$ that contains $n+k = 3+1$ points.

Plugin points...

\[
(1-2)(p_2 + p_1 + p_0) \equiv (3)(1-2) \pmod{7}
\]
\[
(2-2)(4p_2 + 2p_1 + p_0) \equiv (1)(2-2) \pmod{7}
\]
\[
(3-2)(2p_2 + 3p_1 + p_0) \equiv (6)(3-2) \pmod{7}
\]
\[
(4-2)(2p_2 + 4p_1 + p_0) \equiv (0)(4-2) \pmod{7}
\]
\[
(5-2)(4p_2 + 5p_1 + p_0) \equiv (3)(5-2) \pmod{7}
\]

Error locator polynomial: $(x-2)$.

Multiply equation $i$ by $(i-2)$. 

Example.

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

Find \( P(x) = p_2 x^2 + p_1 x + p_0 \) that contains \( n + k = 3 + 1 \) points.

Plugin points...

\[
(1 - 2)(p_2 + p_1 + p_0) \equiv (3)(1 - 2) \pmod{7}
\]

\[
(2 - 2)(4p_2 + 2p_1 + p_0) \equiv (1)(2 - 2) \pmod{7}
\]

\[
(3 - 2)(2p_2 + 3p_1 + p_0) \equiv (6)(3 - 2) \pmod{7}
\]

\[
(4 - 2)(2p_2 + 4p_1 + p_0) \equiv (0)(4 - 2) \pmod{7}
\]

\[
(5 - 2)(4p_2 + 5p_1 + p_0) \equiv (3)(5 - 2) \pmod{7}
\]

Error locator polynomial: \((x - 2)\).

Multiply equation \( i \) by \((i - 2)\). All equations satisfied!
Example.

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

Find \( P(x) = p_2 x^2 + p_1 x + p_0 \) that contains \( n + k = 3 + 1 \) points.

Plugin points...

\[
\begin{align*}
(1 - 2)(p_2 + p_1 + p_0) & \equiv (3)(1 - 2) \pmod{7} \\
(2 - 2)(4p_2 + 2p_1 + p_0) & \equiv (1)(2 - 2) \pmod{7} \\
(3 - 2)(2p_2 + 3p_1 + p_0) & \equiv (6)(3 - 2) \pmod{7} \\
(4 - 2)(2p_2 + 4p_1 + p_0) & \equiv (0)(4 - 2) \pmod{7} \\
(5 - 2)(4p_2 + 5p_1 + p_0) & \equiv (3)(5 - 2) \pmod{7}
\end{align*}
\]

Error locator polynomial: \( (x - 2) \).

Multiply equation \( i \) by \((i - 2)\). All equations satisfied!

But don’t know error locator polynomial!
Example.

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

Find $P(x) = p_2 x^2 + p_1 x + p_0$ that contains $n + k = 3 + 1$ points.

Plugin points...

\[
(1 - 2)(p_2 + p_1 + p_0) \equiv (3)(1 - 2) \pmod{7}
\]
\[
(2 - 2)(4p_2 + 2p_1 + p_0) \equiv (1)(2 - 2) \pmod{7}
\]
\[
(3 - 2)(2p_2 + 3p_1 + p_0) \equiv (6)(3 - 2) \pmod{7}
\]
\[
(4 - 2)(2p_2 + 4p_1 + p_0) \equiv (0)(4 - 2) \pmod{7}
\]
\[
(5 - 2)(4p_2 + 5p_1 + p_0) \equiv (3)(5 - 2) \pmod{7}
\]

Error locator polynomial: $(x - 2)$.

Multiply equation $i$ by $(i - 2)$. All equations satisfied!

But don’t know error locator polynomial! Do know form:
Example.

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

Find $P(x) = p_2 x^2 + p_1 x + p_0$ that contains $n + k = 3 + 1$ points.

Plugin points...

$$(1-2)(p_2 + p_1 + p_0) \equiv (3)(1-2) \pmod{7}$$

$$(2-2)(4p_2 + 2p_1 + p_0) \equiv (1)(2-2) \pmod{7}$$

$$(3-2)(2p_2 + 3p_1 + p_0) \equiv (6)(3-2) \pmod{7}$$

$$(4-2)(2p_2 + 4p_1 + p_0) \equiv (0)(4-2) \pmod{7}$$

$$(5-2)(4p_2 + 5p_1 + p_0) \equiv (3)(5-2) \pmod{7}$$

Error locator polynomial: $(x-2)$.

Multiply equation $i$ by $(i-2)$. All equations satisfied!

But don’t know error locator polynomial! Do know form: $(x-e)$. 
Example.

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

Find $P(x) = p_2 x^2 + p_1 x + p_0$ that contains $n + k = 3 + 1$ points.

Plugin points...

$$
(1 - e)(p_2 + p_1 + p_0) \equiv (3)(1 - e) \pmod{7}
$$
$$
(2 - e)(4p_2 + 2p_1 + p_0) \equiv (1)(2 - e) \pmod{7}
$$
$$
(3 - e)(2p_2 + 3p_1 + p_0) \equiv (3)(3 - e) \pmod{7}
$$
$$
(4 - e)(2p_2 + 4p_1 + p_0) \equiv (0)(4 - e) \pmod{7}
$$
$$
(5 - e)(4p_2 + 5p_1 + p_0) \equiv (3)(5 - e) \pmod{7}
$$

Error locator polynomial: $(x - 2)$.

Multiply equation $i$ by $(i - 2)$. All equations satisfied!

But don’t know error locator polynomial! Do know form: $(x - e)$. 

Example.

Received $R(1) = 3, R(2) = 1, R(3) = 6, R(4) = 0, R(5) = 3$
Find $P(x) = p_2 x^2 + p_1 x + p_0$ that contains $n + k = 3 + 1$ points.

Plugin points...

$$(1 - e)(p_2 + p_1 + p_0) \equiv (3)(1 - e) \pmod{7}$$
$$(2 - e)(4p_2 + 2p_1 + p_0) \equiv (1)(2 - e) \pmod{7}$$
$$(3 - e)(2p_2 + 3p_1 + p_0) \equiv (3)(3 - e) \pmod{7}$$
$$(4 - e)(2p_2 + 4p_1 + p_0) \equiv (0)(4 - e) \pmod{7}$$
$$(5 - e)(4p_2 + 5p_1 + p_0) \equiv (3)(5 - e) \pmod{7}$$

Error locator polynomial: $(x - 2)$.

Multiply equation $i$ by $(i - 2)$. All equations satisfied!

But don’t know error locator polynomial! Do know form: $(x - e)$.

4 unknowns ($p_0, p_1, p_2$ and $e$),
Example.

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

Find $P(x) = p_2 x^2 + p_1 x + p_0$ that contains $n + k = 3 + 1$ points.

Plugin points...

\[
egin{align*}
(1 - e)(p_2 + p_1 + p_0) & \equiv (3)(1 - e) \pmod{7} \\
(2 - e)(4p_2 + 2p_1 + p_0) & \equiv (1)(2 - e) \pmod{7} \\
(3 - e)(2p_2 + 3p_1 + p_0) & \equiv (3)(3 - e) \pmod{7} \\
(4 - e)(2p_2 + 4p_1 + p_0) & \equiv (0)(4 - e) \pmod{7} \\
(5 - e)(4p_2 + 5p_1 + p_0) & \equiv (3)(5 - e) \pmod{7}
\end{align*}
\]

Error locator polynomial: $(x - 2)$.

Multiply equation $i$ by $(i - 2)$. All equations satisfied!

But don’t know error locator polynomial! Do know form: $(x - e)$.

4 unknowns $(p_0, p_1, p_2$ and $e$), 5 nonlinear equations.
..turn their heads each day,

\[(p_{n-1} + \cdots p_0) \equiv R(1) \pmod{p}\]

\[\vdots\]

\[(p_{n-1} i^{n-1} + \cdots p_0) \equiv R(i) \pmod{p}\]

\[\vdots\]

\[(p_{n-1}(n+2k)^{n-1} + \cdots p_0) \equiv R(m) \pmod{p}\]
..turn their heads each day,

\[
E(1)(p_{n-1} + \cdots p_0) \equiv R(1)E(1) \pmod{p} \\
\vdots \\
E(i)(p_{n-1} i^{n-1} + \cdots p_0) \equiv R(i)E(i) \pmod{p} \\
\vdots \\
E(m)(p_{n-1}(n+2k)^{n-1} + \cdots p_0) \equiv R(m)E(m) \pmod{p}
\]

...so satisfied, I’m on my way.
..turn their heads each day,

\[ E(1)(p_{n-1} + \cdots + p_0) \equiv R(1)E(1) \pmod{p} \]

\[ \vdots \]

\[ E(i)(p_{n-1}i^{n-1} + \cdots + p_0) \equiv R(i)E(i) \pmod{p} \]

\[ \vdots \]

\[ E(m)(p_{n-1}(n+2k)^{n-1} + \cdots + p_0) \equiv R(m)E(m) \pmod{p} \]

...so satisfied, I’m on my way.

\( m = n + 2k \) satisfied equations,
..turn their heads each day,

\[
E(1)(p_{n-1} + \cdots p_0) \equiv R(1)E(1) \pmod{p} \\
\vdots \\
E(i)(p_{n-1}i^{n-1} + \cdots p_0) \equiv R(i)E(i) \pmod{p} \\
\vdots \\
E(m)(p_{n-1}(n+2k)^{n-1} + \cdots p_0) \equiv R(m)E(m) \pmod{p}
\]

...so satisfied, I’m on my way.

\[m = n + 2k\] satisfied equations, \(n + k\) unknowns.
..turn their heads each day,

\[
E(1)(p_{n-1} + \cdots p_0) \equiv R(1)E(1) \pmod{p}
\]

\[
E(i)(p_{n-1}i^{n-1} + \cdots p_0) \equiv R(i)E(i) \pmod{p}
\]

\[
E(m)(p_{n-1}(n+2k)^{n-1} + \cdots p_0) \equiv R(m)E(m) \pmod{p}
\]

...so satisfied, I’m on my way.

\[m = n + 2k\] satisfied equations, \[n + k\] unknowns. But nonlinear!
..turn their heads each day,

\[ E(1)(p_{n-1} + \cdots + p_0) \equiv R(1)E(1) \pmod{p} \]

\[ \vdots \]

\[ E(i)(p_{n-1}i^{n-1} + \cdots + p_0) \equiv R(i)E(i) \pmod{p} \]

\[ \vdots \]

\[ E(m)(p_{n-1}(n+2k)^{n-1} + \cdots + p_0) \equiv R(m)E(m) \pmod{p} \]

...so satisfied, I’m on my way.

\[ m = n + 2k \] satisfied equations, \( n + k \) unknowns. But nonlinear!

Let \( Q(x) = E(x)P(x) = a_{n+k-1}x^{n+k-1} + \cdots + a_0 \).
..turn their heads each day,

\[
E(1)(p_{n-1} + \cdots + p_0) \equiv R(1)E(1) \pmod{p}
\]
\[
\vdots
\]
\[
E(i)(p_{n-1}i^{n-1} + \cdots + p_0) \equiv R(i)E(i) \pmod{p}
\]
\[
\vdots
\]
\[
E(m)(p_{n-1}(n+2k)^{n-1} + \cdots + p_0) \equiv R(m)E(m) \pmod{p}
\]

...so satisfied, I’m on my way.

\(m = n + 2k\) satisfied equations, \(n + k\) unknowns. But nonlinear!

Let \(Q(x) = E(x)P(x) = a_{n+k-1}x^{n+k-1} + \cdots + a_0\).

Equations:

\[Q(i) = R(i)E(i).\]
..turn their heads each day,

\[ E(1)(\rho_{n-1} + \cdots \rho_0) \equiv R(1)E(1) \pmod{p} \]

\[ \vdots \]

\[ E(i)(\rho_{n-1}i^{n-1} + \cdots \rho_0) \equiv R(i)E(i) \pmod{p} \]

\[ \vdots \]

\[ E(m)(\rho_{n-1}(n+2k)^{n-1} + \cdots \rho_0) \equiv R(m)E(m) \pmod{p} \]

...so satisfied, I’m on my way.

\( m = n + 2k \) satisfied equations, \( n + k \) unknowns. But nonlinear!

Let \( Q(x) = E(x)P(x) = a_{n+k-1}x^{n+k-1} + \cdots a_0 \).

Equations:

\[ Q(i) = R(i)E(i). \]
..turn their heads each day,

\[ E(1)(p_{n-1} + \cdots + p_0) \equiv R(1)E(1) \pmod{p} \]
\[ \vdots \]
\[ E(i)(p_{n-1}i^{n-1} + \cdots + p_0) \equiv R(i)E(i) \pmod{p} \]
\[ \vdots \]
\[ E(m)(p_{n-1}(n+2k)^{n-1} + \cdots + p_0) \equiv R(m)E(m) \pmod{p} \]

...so satisfied, I’m on my way.

\[ m = n + 2k \] satisfied equations, \( n + k \) unknowns. But nonlinear!

Let \( Q(x) = E(x)P(x) = a_{n+k-1}x^{n+k-1} + \cdots a_0 \).

Equations:

\[ Q(i) = R(i)E(i). \]
 ..turn their heads each day,

\[
E(1)(p_{n-1} + \cdots + p_0) \equiv R(1)E(1) \pmod{p}
\]

\[
\vdots
\]

\[
E(i)(p_{n-1}i^{n-1} + \cdots + p_0) \equiv R(i)E(i) \pmod{p}
\]

\[
\vdots
\]

\[
E(m)(p_{n-1}(n+2k)^{n-1} + \cdots + p_0) \equiv R(m)E(m) \pmod{p}
\]

...so satisfied, I’m on my way.

\(m = n + 2k\) satisfied equations, \(n + k\) unknowns. But nonlinear!

Let \(Q(x) = E(x)P(x) = a_{n+k-1}x^{n+k-1} + \cdots a_0\).

Equations:

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

and linear in \(a_i\) and coefficients of \(E(x)\)!
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 $k$ ...

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

\[ \implies k \text{ (unknown) coefficients.} \]
Finding $Q(x)$ and $E(x)$?

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

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

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

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

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

  $\Rightarrow k$ (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 $k$ ...

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

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

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

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

\[ \implies n + k \text{ (unknown) coefficients.} \]

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.

$$a_{n+k-1} + \cdots + a_0 \equiv R(1)(1 + b_{k-1} \cdots b_0) \pmod{p}$$
For all points 1, \ldots, i, n + 2k,

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

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

\[
\begin{align*}
a_{n+k-1} + \cdots + a_0 & \equiv R(1)(1 + b_{k-1} \cdots b_0) \pmod{p} \\
a_{n+k-1}(2)^{n+k-1} + \cdots + a_0 & \equiv R(2)((2)^k + b_{k-1}(2)^{k-1} \cdots b_0) \pmod{p} \\
& \vdots
\end{align*}
\]
Solving for $Q(x)$ and $E(x)$...

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

$$Q(i) = R(i)E(i) \quad (\text{mod } p)$$

Gives $n + 2k$ linear equations.

\[
\begin{align*}
    a_{n+k-1} + \ldots a_0 & \equiv R(1)(1 + b_{k-1} \cdots b_0) \quad (\text{mod } p) \\
    a_{n+k-1}(2)^{n+k-1} + \ldots a_0 & \equiv R(2)((2)^k + b_{k-1}(2)^{k-1} \cdots b_0) \quad (\text{mod } p) \\
    \vdots \\
    a_{n+k-1}(m)^{n+k-1} + \ldots a_0 & \equiv R(m)((m)^k + b_{k-1}(m)^{k-1} \cdots b_0) \quad (\text{mod } p)
\end{align*}
\]
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 $E(x)$!
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.

\begin{align*}
    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}
\end{align*}

..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.

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

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

$$\vdots$$

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

..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 $P(x) = Q(x)/E(x)$. 
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 $P(x) = Q(x)/E(x)$. 

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

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

Gives $n+2k$ linear equations.

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

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

$$\vdots$$

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

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

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

$E(x) = x - b_0$

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

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

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

$E(x) = x - b_0$

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

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

\[ Q(x) = E(x)P(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0 \]

\[ E(x) = x - b_0 \]

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

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

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

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

$E(x) = x - b_0$

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

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

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

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

Received \( R(1) = 3, R(2) = 1, R(3) = 6, R(4) = 0, R(5) = 3 \)
\[ Q(x) = E(x)P(x) = a_3x^3 + a_2x^2 + a_1x + a_0 \]
\[ E(x) = x - b_0 \]
\[ Q(i) = R(i)E(i). \]

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

\[ a_3 = 1, a_2 = 6, a_1 = 6, a_0 = 5 \text{ and } b_0 = 2. \]
\[ Q(x) = x^3 + 6x^2 + 6x + 5. \]
\[ E(x) = x - 2. \]
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.

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

\[
\begin{array}{c}
\text{-----------------} \\
( x - 2 ) x^3 + 6x^2 + 6x + 5 \\
\text{-----------------} \\
\end{array}
\]

Message is

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

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

What is \( x - 2 \) except at \( x = 2 \)?
Example: finishing up.

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

\[
\begin{array}{l}
\phantom{1} x^2 \\
\hline
x - 2 \quad | \quad x^3 + 6x^2 + 6x + 5 \\
\phantom{x - 2} \; x^3 - 2x^2 \\
\phantom{x^2} \; x^2 - 2x \\
\phantom{x^2} \; x + 5 \\
0
\end{array}
\]
Example: finishing up.

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

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

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

Message is

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

What is \( x - 2 \) except at \( x = 2 \)?

Hole there?
Example: finishing up.

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

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

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

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

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

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

Message is

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

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

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}{cccc}
1 & x^2 & + & 1 \\
\hline
x - 2 & \) & x^3 & + & 6x^2 & + & 6x & + & 5 \\
x^3 & - & 2x^2 & \\
\hline
1 & x^2 & + & 6x & + & 5 \\
1 & x^2 & - & 2x & \\
\hline
x & + & 5 \\
x & - & 2
\end{array}
\]

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

What is \( x - 2 \)?

Except at \( x = 2 \)?

Hole there?
Example: finishing up.

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

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

\[ \frac{P(1)}{P(2)} = 3, \quad \frac{P(3)}{P(2)} = 6. \]

What is \( x - 2 \)?

**Hole there?**
Example: finishing up.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

What is \( \frac{x-2}{x-2} \)? 1 Except at \( x = 2 \)? 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.
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.
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.
Is there one and only one $P(x)$ from Berlekamp-Welsh procedure?
Hmmm...

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

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

**Proof:**

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

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

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

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

$$\frac{Q'(x)}{E'(x)} = \frac{Q(x)}{E(x)} = P(x).$$  \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:
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 $n + 2k - 1$
**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

$$Q'(x)E(x) = Q(x)E'(x)$$
on $n + 2k$ 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.
Unique solution for $P(x)$

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

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

**Proof:**

We claim

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

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

**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 \( n+2k-1 \)

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

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

Can cross divide at \( n \) points.

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

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

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

(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

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

(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.

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

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

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

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

**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.

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

Both degree $\leq n$ $\Rightarrow$ Same polynomial! 

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

$Q'(x)E(x) = Q(x)E'(x)$ holds when $E(x)$ or $E'(x)$ are zero.

When $E'(x)$ and $E(x)$ are not zero, $Q'(x)E'(x) = Q(x)E(x) = R(x)$.

Cross multiplying gives equality in fact for these points. Points to polynomials, have to deal with zeros!

Example: dealing with $x - 2x - 2$ at $x = 2$. 
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 $Q'(i) = 0$. 

Cross multiplying gives equality in fact for these points.

Points to polynomials, have to deal with zeros!

Example: dealing with $x^2 - 2x - 2$ at $x = 2$. 

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

Proof: Construction implies that

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

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

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

\[
\Rightarrow Q(i)E'(i) = Q'(i)E(i) \text{ holds when } E(i) \text{ or } E'(i) \text{ are zero.}
\]
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 $Q'(i) = 0$.

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

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

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

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

\[\Rightarrow\] \( Q(i)E'(i) = Q'(i)E(i) \) 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 $Q'(i) = 0$.

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

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.
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. \( \square \)
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. Error Correction.

Communicate \( n \) packets, with \( k \) erasures.
Summary. Error Correction.

Communicate \( n \) packets, with \( k \) erasures.

How many packets?
Summary. Error Correction.

Communicate \(n\) packets, with \(k\) erasures.

How many packets? \(n + k\)
Summary. Error Correction.

Communicate $n$ packets, with $k$ erasures.

How many packets? $n + k$
How to encode?

---

Reed-Solomon codes.
Welsh-Berlekamp Decoding.
Perfection!
Communicate $n$ packets, with $k$ erasures.

How many packets? $n + k$
How to encode? With polynomial, $P(x)$. 
Summary. Error Correction.

Communicate \( n \) packets, with \( k \) erasures.

How many packets? \( n + k \)
How to encode? With polynomial, \( P(x) \).
Of degree?
Summary. Error Correction.

Communicate \( n \) packets, with \( k \) erasures.

- How many packets? \( n + k \)
- How to encode? With polynomial, \( P(x) \).
- Of degree? \( n - 1 \)
Summary. Error Correction.

Communicate $n$ packets, with $k$ erasures.

How many packets? $n + k$
How to encode? With polynomial, $P(x)$.
Of degree? $n - 1$
Recover?
Summary. Error Correction.

Communicate \( n \) packets, with \( k \) erasures.

- How many packets? \( n + k \)
- How to encode? With polynomial, \( P(x) \).
- Of degree? \( n - 1 \)
- Recover? Reconstruc\( t \) \( P(x) \) with any \( n \) points!
Summary. Error Correction.

Communicate $n$ packets, with $k$ erasures.

How many packets? $n + k$
How to encode? With polynomial, $P(x)$.
Of degree? $n - 1$
Recover? Reconstruct $P(x)$ with any $n$ points!

Communicate $n$ packets, with $k$ errors.
Summary. Error Correction.

Communicate $n$ packets, with $k$ erasures.

How many packets? $n + k$
How to encode? With polynomial, $P(x)$.
Of degree? $n - 1$
Recover? Reconstruct $P(x)$ with any $n$ points!

Communicate $n$ packets, with $k$ errors.

How many packets?
Summary. Error Correction.

Communicate $n$ packets, with $k$ erasures.

- How many packets? $n + k$
- How to encode? With polynomial, $P(x)$.
- Of degree? $n - 1$
- Recover? Reconstruct $P(x)$ with any $n$ points!

Communicate $n$ packets, with $k$ errors.

- How many packets? $n + 2k$
Summary. Error Correction.

Communicate \( n \) packets, with \( k \) erasures.

- How many packets? \( n + k \)
- How to encode? With polynomial, \( P(x) \).
- Of degree? \( n - 1 \)
- Recover? Reconstruct \( P(x) \) with any \( n \) points!

Communicate \( n \) packets, with \( k \) errors.

- How many packets? \( n + 2k \)
- Why?
Summary. Error Correction.

Communicate \( n \) packets, with \( k \) erasures.

- How many packets? \( n + k \)
- How to encode? With polynomial, \( P(x) \).
- Of degree? \( n - 1 \)
- Recover? Reconstruct \( P(x) \) with any \( n \) points!

Communicate \( n \) packets, with \( k \) errors.

- How many packets? \( n + 2k \)
- Why?
  - \( k \) changes to make diff. messages overlap
Summary. Error Correction.

Communicate $n$ packets, with $k$ erasures.

How many packets? $n + k$
How to encode? With polynomial, $P(x)$.
Of degree? $n - 1$
Recover? Reconstruct $P(x)$ with any $n$ points!

Communicate $n$ packets, with $k$ errors.

How many packets? $n + 2k$
Why?
   $k$ changes to make diff. messages overlap
How to encode?
Summary. Error Correction.

Communicate $n$ packets, with $k$ erasures.

How many packets? $n + k$
How to encode? With polynomial, $P(x)$.
Of degree? $n - 1$
Recover? Reconstruct $P(x)$ with any $n$ points!

Communicate $n$ packets, with $k$ errors.

How many packets? $n + 2k$
Why?
   $k$ changes to make diff. messages overlap
How to encode? With polynomial, $P(x)$. 
Summary. Error Correction.

Communicate $n$ packets, with $k$ erasures.

How many packets? $n + k$
How to encode? With polynomial, $P(x)$.
Of degree? $n - 1$
Recover? Reconstruct $P(x)$ with any $n$ points!

Communicate $n$ packets, with $k$ errors.

How many packets? $n + 2k$
Why?
  $k$ changes to make diff. messages overlap
How to encode? With polynomial, $P(x)$. Of degree?
Summary. Error Correction.

Communicate $n$ packets, with $k$ erasures.

- How many packets? $n + k$
- How to encode? With polynomial, $P(x)$.
- Of degree? $n - 1$
- Recover? Reconstruct $P(x)$ with any $n$ points!

Communicate $n$ packets, with $k$ errors.

- How many packets? $n + 2k$
- Why?
  - $k$ changes to make diff. messages overlap
Summary. Error Correction.

Communicate $n$ packets, with $k$ erasures.

- How many packets? $n + k$
- How to encode? With polynomial, $P(x)$.
- Of degree? $n - 1$
- Recover? Reconstruct $P(x)$ with any $n$ points!

Communicate $n$ packets, with $k$ errors.

- How many packets? $n + 2k$
- Why?
  - $k$ changes to make diff. messages overlap
- Recover?
Summary. Error Correction.

Communicate $n$ packets, with $k$ erasures.

How many packets? $n + k$
How to encode? With polynomial, $P(x)$.
Of degree? $n - 1$
Recover? Reconstruct $P(x)$ with any $n$ points!

Communicate $n$ packets, with $k$ errors.

How many packets? $n + 2k$
Why?
  $k$ changes to make diff. messages overlap
How to encode? With polynomial, $P(x)$. Of degree? $n - 1$.
Recover?
Summary. Error Correction.

Communicate $n$ packets, with $k$ erasures.

- How many packets? $n + k$
- How to encode? With polynomial, $P(x)$.
- Of degree? $n - 1$
- Recover? Reconstruct $P(x)$ with any $n$ points!

Communicate $n$ packets, with $k$ errors.

- How many packets? $n + 2k$
- Why?
  - $k$ changes to make diff. messages overlap
- Recover?
  - Reconstruct error polynomial, $E(X)$, and $P(x)$!
Summary. Error Correction.

Communicate $n$ packets, with $k$ erasures.

- How many packets? $n + k$
- How to encode? With polynomial, $P(x)$.
- Of degree? $n - 1$
- Recover? Reconstruct $P(x)$ with any $n$ points!

Communicate $n$ packets, with $k$ errors.

- How many packets? $n + 2k$
- Why?
  - $k$ changes to make diff. messages overlap
- Recover?
  - Reconstruct error polynomial, $E(X)$, and $P(x)$!
    - Nonlinear equations.
Summary. Error Correction.

Communicate \( n \) packets, with \( k \) erasures.

- How many packets? \( n + k \)
- How to encode? With polynomial, \( P(x) \).
- Of degree? \( n - 1 \)
- Recover? Reconstruct \( P(x) \) with any \( n \) points!

Communicate \( n \) packets, with \( k \) errors.

- How many packets? \( n + 2k \)
- Why?
  - \( k \) changes to make diff. messages overlap
- How to encode? With polynomial, \( P(x) \). Of degree? \( n - 1 \).
- Recover?
  - Reconstruct error polynomial, \( E(X) \), and \( P(x) \)!
  - Nonlinear equations.
  - Reconstruct \( E(x) \) and \( Q(x) = E(x)P(x) \).
Summary. Error Correction.

Communicate $n$ packets, with $k$ erasures.

- How many packets? $n + k$
- How to encode? With polynomial, $P(x)$.
- Of degree? $n - 1$
- Recover? Reconstruct $P(x)$ with any $n$ points!

Communicate $n$ packets, with $k$ errors.

- How many packets? $n + 2k$
- Why?
  - $k$ changes to make diff. messages overlap
- Recover?
  - Reconstruct error polynomial, $E(X)$, and $P(x)$!
    - Nonlinear equations.
  - Reconstruct $E(x)$ and $Q(x) = E(x)P(x)$. Linear Equations.
Summary. Error Correction.

Communicate \( n \) packets, with \( k \) erasures.

- How many packets? \( n + k \)
- How to encode? With polynomial, \( P(x) \).
- Of degree? \( n - 1 \)
- Recover? Reconstruct \( P(x) \) with any \( n \) points!

Communicate \( n \) packets, with \( k \) errors.

- How many packets? \( n + 2k \)
- Why?
  - \( k \) changes to make diff. messages overlap
- How to encode? With polynomial, \( P(x) \). Of degree? \( n - 1 \).
- Recover?
  - Reconstruct error polynomial, \( E(X) \), and \( P(x) \)!
    - Nonlinear equations.
  - Reconstruct \( E(x) \) and \( Q(x) = E(x)P(x) \). Linear Equations.
  - Polynomial division!
Summary. Error Correction.

Communicate $n$ packets, with $k$ erasures.

- How many packets? $n + k$
- How to encode? With polynomial, $P(x)$.
- Of degree? $n - 1$
- Recover? Reconstruct $P(x)$ with any $n$ points!

Communicate $n$ packets, with $k$ errors.

- How many packets? $n + 2k$
- Why?
  - $k$ changes to make diff. messages overlap
- Recover?
  - Reconstruct error polynomial, $E(X)$, and $P(x)$!
    - **Nonlinear equations.**
  - Reconstruct $E(x)$ and $Q(x) = E(x)P(x)$. Linear Equations.
  - Polynomial division! $P(x) = Q(x)/E(x)$!
Summary. Error Correction.

Communicate $n$ packets, with $k$ erasures.

- How many packets? $n + k$
- How to encode? With polynomial, $P(x)$.
- Of degree? $n - 1$
- Recover? Reconstruct $P(x)$ with any $n$ points!

Communicate $n$ packets, with $k$ errors.

- How many packets? $n + 2k$
- Why?
  - $k$ changes to make diff. messages overlap
- Recover?
  - Reconstruct error polynomial, $E(X)$, and $P(x)$!
    - Nonlinear equations.
  - Reconstruct $E(x)$ and $Q(x) = E(x)P(x)$. Linear Equations.
    - Polynomial division! $P(x) = Q(x)/E(x)$!

Reed-Solomon codes.
Summary. Error Correction.

Communicate \( n \) packets, with \( k \) erasures.

- How many packets? \( n + k \)
- How to encode? With polynomial, \( P(x) \).
- Of degree? \( n - 1 \)
- Recover? Reconstruct \( P(x) \) with any \( n \) points!

Communicate \( n \) packets, with \( k \) errors.

- How many packets? \( n + 2k \)
- Why?
  - \( k \) changes to make diff. messages overlap
- How to encode? With polynomial, \( P(x) \). Of degree? \( n - 1 \).
- Recover?
  - Reconstruct error polynomial, \( E(X) \), and \( P(x) \)!
    - Nonlinear equations.
  - Reconstruct \( E(x) \) and \( Q(x) = E(x)P(x) \). Linear Equations.
    - Polynomial division! \( P(x) = Q(x)/E(x) \)!

Reed-Solomon codes. Welsh-Berlekamp Decoding.
Summary. Error Correction.

Communicate \( n \) packets, with \( k \) erasures.

How many packets? \( n + k \)
How to encode? With polynomial, \( P(x) \).
Of degree? \( n - 1 \)
Recover? Reconstruct \( P(x) \) with any \( n \) points!

Communicate \( n \) packets, with \( k \) errors.

How many packets? \( n + 2k \)
Why?
    \( k \) changes to make diff. messages overlap
How to encode? With polynomial, \( P(x) \). Of degree? \( n - 1 \).
Recover?
    Reconstruct error polynomial, \( E(X) \), and \( P(x) \)!
    Nonlinear equations.
Reconstruct \( E(x) \) and \( Q(x) = E(x)P(x) \). Linear Equations.
    Polynomial division! \( P(x) = Q(x)/E(x) \)!

Reed-Solomon codes. Welsh-Berlekamp Decoding. Perfection!