Secret Sharing
Problem of (2, 2)- Secret Sharing

Zelda has a secret \( s \in \mathbb{N} \).
Problem of (2, 2)-Secret Sharing

Zelda has a secret $s \in \mathbb{N}$.
Zelda has two friends Alice and Bob who do not get along.
Problem of (2, 2)- Secret Sharing

Zelda has a secret \( s \in \mathbb{N} \).
Zelda has two friends Alice and Bob who do not get along.
Zelda wants to give each of them a natural number so that:

1. If Alice and Bob get together then they can learn \( s \).
2. Alice alone does not know anything about \( s \).
3. Bob alone does not know anything about \( s \).

This is called (2, 2)-secret sharing since you need 2 out of the 2 to cooperate.
Zelda has a secret $s \in \mathbb{N}$. 
Zelda has two friends Alice and Bob who do not get along. 
Zelda wants to give each of them a natural number so that:

1. If Alice and Bob get together then they can learn $s$.

This is called $(2, 2)$-secret sharing since you need 2 out of the 2 to cooperate.
Problem of $(2, 2)$- Secret Sharing

Zelda has a secret $s \in \mathbb{N}$.

Zelda has two friends Alice and Bob who do not get along. Zelda wants to give each of them a natural number so that:

1. If Alice and Bob get together then they can learn $s$.
2. Alice alone does not know anything about $s$.
3. Bob alone does not know anything about $s$.

This is called $(2, 2)$-secret sharing since you need 2 out of the 2 to cooperate.
Problem of \((2, 2)\)-Secret Sharing

Zelda has a secret \(s \in \mathbb{N}\).

Zelda has two friends Alice and Bob who do not get along. Zelda wants to give each of them a natural number so that:

1. If Alice and Bob get together then they can learn \(s\).
2. Alice alone does not know anything about \(s\).
3. Bob alone does not know anything about \(s\).
Problem of (2, 2)- Secret Sharing

Zelda has a secret $s \in \mathbb{N}$.
Zelda has two friends Alice and Bob who do not get along. Zelda wants to give each of them a natural number so that:

1. If Alice and Bob get together then they can learn $s$.
2. Alice alone does not know anything about $s$.
3. Bob alone does not know anything about $s$.

This is called (2, 2)-secret sharing since you need 2 out of the 2 to cooperate.
An Attempt at (2, 2)-Secret Sharing

1. Say $s$ is not prime so $s = s_1 s_2$.

2. Zelda gives Alice $s_1$.

3. Zelda gives Bob $s_2$.

Does this work?

1. If Alice and Bob get together they can find $s_1 s_2 = s$.

   YEAH.

2. Alice knows a factor of $s$.

   BOO.

   This is bad. We want Alice and Bob do learn nothing unless they get together.
1. Say $s$ is not prime so $s = s_1s_2$. 

2. Zelda gives Alice $s_1$.

3. Zelda gives Bob $s_2$.

Does this work?

1. If Alice and Bob get together they can find $s_1s_2 = s$.

YEAH.

2. Alice knows a factor of $s$.

BOO.

This is bad. We want Alice and Bob to learn nothing unless they get together.
An Attempt at $(2, 2)$-Secret Sharing

1. Say $s$ is not prime so $s = s_1 s_2$.
2. Zelda gives Alice $s_1$. 

1. If Alice and Bob get together they can find $s_1 s_2 = s$.

YEAH.

2. Alice knows a factor of $s$.

BOO.

This is bad. We want Alice and Bob to learn nothing unless they get together.
An Attempt at (2, 2)-Secret Sharing

1. Say $s$ is not prime so $s = s_1s_2$.
2. Zelda gives Alice $s_1$.
3. Zelda gives Bob $s_2$. 

Does this work?

1. If Alice and Bob get together they can find $s_1s_2 = s$.
   YEAH.
2. Alice knows a factor of $s$.
   BOO.

This is bad. We want Alice and Bob do learn nothing unless they get together.
An Attempt at (2, 2)-Secret Sharing

1. Say $s$ is not prime so $s = s_1 s_2$.
2. Zelda gives Alice $s_1$.
3. Zelda gives Bob $s_2$.

Does this work?
An Attempt at (2, 2)-Secret Sharing

1. Say $s$ is not prime so $s = s_1s_2$.
2. Zelda gives Alice $s_1$.
3. Zelda gives Bob $s_2$.

Does this work?

1. If Alice and Bob get together they can find $s_1s_2 = s$. 
An Attempt at (2, 2)-Secret Sharing

1. Say $s$ is not prime so $s = s_1 s_2$.
2. Zelda gives Alice $s_1$.
3. Zelda gives Bob $s_2$.

Does this work?

1. If Alice and Bob get together they can find $s_1 s_2 = s$. **YEAH.**
An Attempt at (2, 2)-Secret Sharing

1. Say $s$ is not prime so $s = s_1 s_2$.
2. Zelda gives Alice $s_1$.
3. Zelda gives Bob $s_2$.

Does this work?

1. If Alice and Bob get together they can find $s_1 s_2 = s$. **YEAH.**
2. Alice knows a factor of $s$. 
An Attempt at (2, 2)-Secret Sharing

1. Say $s$ is not prime so $s = s_1 s_2$.
2. Zelda gives Alice $s_1$.
3. Zelda gives Bob $s_2$.

Does this work?

1. If Alice and Bob get together they can find $s_1 s_2 = s$. **YEAH.**
2. Alice knows a factor of $s$. **BOO.**
An Attempt at \((2, 2)\)-Secret Sharing

1. Say \(s\) is not prime so \(s = s_1 s_2\).
2. Zelda gives Alice \(s_1\).
3. Zelda gives Bob \(s_2\).

Does this work?

1. If Alice and Bob get together they can find \(s_1 s_2 = s\). \textbf{YEAH}.
2. Alice knows a factor of \(s\). \textbf{BOO}.

This is bad. We want Alice and Bob do learn \textbf{nothing} unless they get together.
Solution to (2, 2)-Secret Sharing

1. Zelda has a secret $s \in \mathbb{N}$.
2. Zelda picks a random natural number $r$. Let $f(x) = rx + s$.
3. Zelda gives Alice $f(1)$.
4. Zelda gives Bob $f(2)$.

If Alice and Bob get together, they know 2 points on the line $f$, hence they can find the equation for $f$, and hence $s$.

Alice alone just knows $f(1)$. From this she cannot deduce anything about $s$. 

Solution to (2, 2)-Secret Sharing

1. Zelda has a secret $s \in \mathbb{N}$. 
Solution to (2, 2)-Secret Sharing

1. Zelda has a secret \( s \in \mathbb{N} \).
2. Zelda picks a random natural number \( r \). Let \( f \) be

\[
    f(x) = rx + s.
\]
1. Zelda has a secret $s \in \mathbb{N}$.

2. Zelda picks a random natural number $r$. Let $f$ be

$$f(x) = rx + s.$$ 

3. Zelda gives Alice $f(1)$.
Solution to (2, 2)-Secret Sharing

1. Zelda has a secret $s \in \mathbb{N}$.
2. Zelda picks a random natural number $r$. Let $f$ be

   $$f(x) = rx + s.$$  

3. Zelda gives Alice $f(1)$.
4. Zelda gives Bob $f(2)$.
Solution to \((2, 2)\)-Secret Sharing

1. Zelda has a secret \(s \in \mathbb{N}\).
2. Zelda picks a random natural number \(r\). Let \(f\) be

\[ f(x) = rx + s. \]

3. Zelda gives Alice \(f(1)\).
4. Zelda gives Bob \(f(2)\).

If Alice and Bob get together they know 2 points on the line \(f\), hence they can find the equation for \(f\), and hence \(s\).
Solution to (2, 2)-Secret Sharing

1. Zelda has a secret $s \in \mathbb{N}$.
2. Zelda picks a random natural number $r$. Let $f$ be
   
   $$f(x) = rx + s.$$  

3. Zelda gives Alice $f(1)$.
4. Zelda gives Bob $f(2)$.

If Alice and Bob get together they know 2 points on the line $f$, hence they can find the equation for $f$, and hence $s$. Alice alone just knows $f(1)$. From this she cannot deduce anything about $s$. 
Example

Zelda’s secret is 13.
Example

Zelda’s secret is 13.
Zelda picks random number 3.
Example

Zelda’s secret is 13.
Zelda picks random number 3.
f is

\[ f(x) = 3x + 13. \]
Example

Zelda’s **secret** is 13.
Zelda picks random number 3.

\[ f \] is

\[ f(x) = 3x + 13. \]

Zelda gives Alice \( f(1) = 16 \).
Zelda’s secret is 13.
Zelda picks random number 3.

\[ f(x) = 3x + 13. \]

Zelda gives Alice \( f(1) = 16 \).
Zelda gives Bob \( f(2) = 19 \).
Example

Zelda’s secret is 13.
Zelda picks random number 3.
f is

\[ f(x) = 3x + 13. \]

Zelda gives Alice \( f(1) = 16 \).
Zelda gives Bob \( f(2) = 19 \).
If Alice and Bob get together they know that \( (1, 16) \) and \( (2, 19) \) are on the line \( f \), so they can find the equation for \( f \), and hence \( s \).
Example

Zelda’s secret is 13.
Zelda picks random number 3.
f is

\[ f(x) = 3x + 13. \]

Zelda gives Alice \( f(1) = 16 \).
Zelda gives Bob \( f(2) = 19 \).
If Alice and Bob get together they know that \( (1, 16) \) and \( (2, 19) \)
are on the line \( f \), so they can find the equation for \( f \), and hence \( s \).
Alice alone just knows that \( (1, 16) \) is on the line. Tells her nothing
about the constant term \( s \).
Problem of (3, 3)-Secret Sharing

Zelda has a secret $s \in \mathbb{N}$. 
Problem of $(3, 3)$-Secret Sharing

Zelda has a secret $s \in \mathbb{N}$.

Zelda has three friends Alice, Bob, Carol who do not get along.
Problem of $(3,3)$-Secret Sharing

Zelda has a secret $s \in \mathbb{N}$.

Zelda has three friends Alice, Bob, Carol who do not get along. Zelda wants to give each of them a natural number so that

1. If all three get together then they can learn $s$.
2. If any two get together they do not learn anything about $s$.
Problem of $(3, 3)$-Secret Sharing

Zelda has a secret $s \in \mathbb{N}$.

Zelda has three friends Alice, Bob, Carol who do not get along. Zelda wants to give each of them a natural number so that

1. If all three get together then they can learn $s$.

2. If any two get together they do not learn anything about $s$.

Discuss how this can be done.
Zelda has a secret $s \in \mathbb{N}$.

Zelda has three friends Alice, Bob, Carol who do not get along. Zelda wants to give each of them a natural number so that

1. If all three get together then they can learn $s$.
2. If any two get together they do not learn anything about $s$. 

Problem of $(3, 3)$-Secret Sharing
Problem of (3, 3)-Secret Sharing

Zelda has a secret $s \in \mathbb{N}$.
Zelda has three friends Alice, Bob, Carol who do not get along.
Zelda wants to give each of them a natural number so that
1. If all three get together then they can learn $s$.
2. If any two get together they do not learn anything about $s$.
Discuss how this can be done.
Solution to $(3, 3)$-Secret Sharing

1. Zelda has a secret $s \in \mathbb{N}$.
2. Zelda picks random natural numbers $r_1, r_2$. Let $f(x) = r_1x^2 + r_2x + s$.
3. Zelda gives Alice $f(1)$, gives Bob $f(2)$, gives Carol $f(3)$.

If all three get together they have 3 points on the quadratic $f$, hence can find the equation for $f$, and hence $s$. If any two get together they don't learn anything about $s$. 
Solution to (3, 3)-Secret Sharing

1. Zelda has a secret $s \in \mathbb{N}$. 
Solution to \((3, 3)\)-Secret Sharing

1. Zelda has a secret \(s \in \mathbb{N}\).
2. Zelda picks random natural numbers \(r_1, r_2\). Let \(f\) be

\[
f(x) = r_1 x^2 + r_2 x + s.
\]
Solution to \((3,3)\)-Secret Sharing

1. Zelda has a secret \(s \in \mathbb{N}\).
2. Zelda picks random natural numbers \(r_1, r_2\). Let \(f\) be
   \[
   f(x) = r_1 x^2 + r_2 x + s.
   \]
3. Zelda gives Alice \(f(1)\), gives Bob \(f(2)\), gives Carol \(f(3)\).
Solution to (3, 3)-Secret Sharing

1. Zelda has a secret $s \in \mathbb{N}$.
2. Zelda picks random natural numbers $r_1, r_2$. Let $f$ be

$$f(x) = r_1 x^2 + r_2 x + s.$$ 

3. Zelda gives Alice $f(1)$, gives Bob $f(2)$, gives Carol $f(3)$. If all three get together they have 3 points on the quadratic $f$, hence can find the equation for $f$, and hence $s$. 
Solution to (3, 3)-Secret Sharing

1. Zelda has a secret $s \in \mathbb{N}$.

2. Zelda picks random natural numbers $r_1, r_2$. Let $f$ be

   $$f(x) = r_1 x^2 + r_2 x + s.$$ 

3. Zelda gives Alice $f(1)$, gives Bob $f(2)$, gives Carol $f(3)$.
   
   If all three get together they have 3 points on the quadratic $f$, hence can find the equation for $f$, and hence $s$.
   
   If any two get together they don’t learn anything about $s$. 
Another Solution to $(3, 3)$-Secret Sharing

The solution to $(3, 3)$-Secret Sharing used 3 Points in $R^2$ to determine a Quadratic. There is an alternative solution that uses 3 Points in $R^3$ to determine a Plane.
Another Solution to (3, 3)-Secret Sharing

The solution to (3, 3)-Secret Sharing used

3 Points in $\mathbb{R}^2$ Determine a Quadratic
Another Solution to (3, 3)-Secret Sharing

The solution to (3, 3)-Secret Sharing used

3 Points in $\mathbb{R}^2$ Determine a Quadratic

There is an alternative solution that uses

3 Points $\mathbb{R}^3$ Determine a Plane
Problem of (4, 7)-Secret Sharing

Zelda has a secret $s \in \mathbb{N}$.
Problem of (4, 7)-Secret Sharing

Zelda has a secret \( s \in \mathbb{N} \).
Zelda has 7 friends \( A_1, \ldots, A_7 \).
Problem of \((4, 7)\)-Secret Sharing

Zelda has a secret \(s \in \mathbb{N}\).

Zelda has 7 friends \(A_1, \ldots, A_7\).

\(A_1, \ldots, A_7\) do not get along.
Problem of \((4, 7)\)-Secret Sharing

Zelda has a secret \(s \in \mathbb{N}\).

Zelda has 7 friends \(A_1, \ldots, A_7\).

\(A_1, \ldots, A_7\) do not get along.

Zelda wants to give each of them a natural number so that

1. If any 4 get together then they can learn \(s\).
2. If any 3 get together they do not learn anything about \(s\).
Problem of (4, 7)-Secret Sharing

Zelda has a secret $s \in \mathbb{N}$.
Zelda has 7 friends $A_1, \ldots, A_7$.
$A_1, \ldots, A_7$ do not get along.
Zelda wants to give each of them a natural number so that
1. If any 4 get together then they can learn $s$.
Zelda has a secret $s \in \mathbb{N}$. 
Zelda has 7 friends $A_1, \ldots, A_7$. 
$A_1, \ldots, A_7$ do not get along. 
Zelda wants to give each of them a natural number so that 
1. If any 4 get together then they can learn $s$. 
2. If any 3 get together they do not learn anything about $s$. 

Problem of $(4, 7)$-Secret Sharing
Problem of (4, 7)-Secret Sharing

Zelda has a secret $s \in \mathbb{N}$.  
Zelda has 7 friends $A_1, \ldots, A_7$.  
$A_1, \ldots, A_7$ do not get along.  
Zelda wants to give each of them a natural number so that  
1. If any 4 get together then they can learn $s$.  
2. If any 3 get together they do not learn anything about $s$.  
Discuss how this can be done.
Solution to (4, 7)-Secret Sharing

1. Zelda has a secret \( s \in \mathbb{N} \).

2. Zelda picks random natural numbers \( r_1, r_2, r_3 \). Let \( f(x) = r_3x^3 + r_2x^2 + r_1x + s \).

3. Zelda gives \( A_1 f(1), A_2 f(2), \ldots, A_7 f(7) \).

If any 4 get together they have 4 points on the cubic \( f \), hence can find the equation for \( f \) and hence \( s \).

If any 3 get together they don't learn anything about \( s \).
Solution to (4, 7)-Secret Sharing

1. Zelda has a secret $s \in \mathbb{N}$.
Solution to (4, 7)-Secret Sharing

1. Zelda has a **secret** $s \in \mathbb{N}$.

2. Zelda picks random natural numbers $r_1, r_2, r_3$. Let $f$ be

   $$f(x) = r_3x^3 + r_2x^2 + r_1x + s.$$
Solution to (4, 7)-Secret Sharing

1. Zelda has a secret $s \in \mathbb{N}$.

2. Zelda picks random natural numbers $r_1, r_2, r_3$. Let $f$ be

$$f(x) = r_3x^3 + r_2x^2 + r_1x + s.$$ 

3. Zelda gives $A_1 f(1), A_2 f(2), \ldots, A_7 f(7)$.

If any 4 get together they have 4 points on the cubic $f$, hence can find the equation for $f$ and hence $s$. If any 3 get together they don't learn anything about $s$. 
Solution to (4, 7)-Secret Sharing

1. Zelda has a secret $s \in \mathbb{N}$.
2. Zelda picks random natural numbers $r_1, r_2, r_3$. Let $f$ be
   \[ f(x) = r_3x^3 + r_2x^2 + r_1x + s. \]
3. Zelda gives $A_1 f(1), A_2 f(2), \ldots, A_7 f(7)$.
   If any 4 get together they have 4 points on the cubic $f$, hence can find the equation for $f$ and hence $s$. 
Solution to (4, 7)-Secret Sharing

1. Zelda has a **secret** \( s \in \mathbb{N} \).
2. Zelda picks random natural numbers \( r_1, r_2, r_3 \). Let \( f \) be

\[
f(x) = r_3x^3 + r_2x^2 + r_1x + s.
\]

3. Zelda gives \( A_1 \ f(1), A_2 \ f(2), \ldots, A_7 \ f(7) \).
   If any 4 get together they have 4 points on the cubic \( f \), hence can find the equation for \( f \) and hence \( s \).
   If any 3 get together they don’t learn **anything** about \( s \).
Problem of \((t, m)\)-Secret Sharing

Zelda has a secret \(s \in \mathbb{N}\).
Problem of \((t,m)\)-Secret Sharing

Zelda has a secret \(s \in \mathbb{N}\).

Zelda has \(m\) friends \(A_1, \ldots, A_m\).
Problem of \((t, m)\)-Secret Sharing

Zelda has a secret \(s \in \mathbb{N}\).

Zelda has \(m\) friends \(A_1, \ldots, A_m\).

Zelda wants to give each of them a natural number so that
Problem of \((t,m)\)-Secret Sharing

Zelda has a **secret** \(s \in \mathbb{N}\).

Zelda has \(m\) friends \(A_1, \ldots, A_m\).

Zelda wants to give each of them a natural number so that

1. If any \(t\) get together then they can learn \(s\).
Problem of \((t, m)\)-Secret Sharing

Zelda has a secret \(s \in \mathbb{N}\).

Zelda has \(m\) friends \(A_1, \ldots, A_m\).

Zelda wants to give each of them a natural number so that

1. If any \(t\) get together then they can learn \(s\).

2. If any \(t - 1\) get together they do not learn anything about \(s\).
Problem of \((t, m)\)-Secret Sharing

Zelda has a secret \(s \in \mathbb{N}\).
Zelda has \(m\) friends \(A_1, \ldots, A_m\).
Zelda wants to give each of them a natural number so that

1. If any \(t\) get together then they can learn \(s\).
2. If any \(t - 1\) get together they do not learn anything about \(s\).

Discuss how this can be done.
Solution to \((t, m)\)-Secret Sharing

1. Zelda has a secret \(s \in \mathbb{N}\).

2. Zelda picks random natural numbers \(r_1, \ldots, r_{t-1}\). Let 
   \[ f(x) = r_{t-1}x^{t-1} + \cdots + r_1x + s. \]

3. Zelda gives \(A_1 f(1), A_2 f(2), \ldots, A_m f(m)\).

   If any \(t\) get together they have \(t\) points on a \((t-1)\)-degree curve \(f\), hence can find the equation for \(f\), and hence \(s\).

   If any \(t-1\) get together they don't learn anything about \(s\).
1. Zelda has a secret $s \in \mathbb{N}$. 

**Solution to $(t, m)$-Secret Sharing**
Solution to \((t, m)\)-Secret Sharing

1. Zelda has a secret \(s \in \mathbb{N}\).
2. Zelda picks random natural numbers \(r_1, \ldots, r_{t-1}\). Let \(f\) be

\[
f(x) = r_{t-1}x^{t-1} + \cdots + r_1x + s.
\]
Solution to \((t, m)\)-Secret Sharing

1. Zelda has a secret \(s \in \mathbb{N}\).
2. Zelda picks random natural numbers \(r_1, \ldots, r_{t-1}\). Let \(f\) be
   \[ f(x) = r_{t-1}x^{t-1} + \cdots + r_1x + s. \]
3. Zelda gives \(A_1 f(1), A_2 f(2), \ldots, A_m f(m)\).
Solution to $(t, m)$-Secret Sharing

1. Zelda has a secret $s \in \mathbb{N}$.
2. Zelda picks random natural numbers $r_1, \ldots, r_{t-1}$. Let $f$ be
   \[ f(x) = r_{t-1}x^{t-1} + \cdots + r_1x + s. \]
3. Zelda gives $A_1 f(1), A_2 f(2), \ldots, A_m f(m)$.
   If any $t$ get together they have $t$ points on a $t - 1$-degree-curve $f$, hence can find the equation for $f$, and hence $s$. 
Solution to \((t, m)\)-Secret Sharing

1. Zelda has a **secret** \(s \in \mathbb{N}\).

2. Zelda picks random natural numbers \(r_1, \ldots, r_{t-1}\). Let \(f\) be
   \[
   f(x) = r_{t-1}x^{t-1} + \cdots + r_1x + s.
   \]

3. Zelda gives \(A_1 f(1), A_2 f(2), \ldots, A_m f(m)\).
   If any \(t\) get together they have \(t\) points on a \(t - 1\)-degree-curve \(f\), hence can find the equation for \(f\), and hence \(s\).
   If any \(t - 1\) get together they don’t learn **anything** about \(s\).
What I told You is Not Quite Right

The basic ideas I showed you were sound.
What I told You is Not Quite Right

The basic ideas I showed you were sound.
But there is a problem with the protocols I showed you.
What I told You is Not Quite Right

The basic ideas I showed you were sound.
But there is a problem with the protocols I showed you.

How do you pick a Random Natural?
What I told You is Not Quite Right

The basic ideas I showed you were sound. But there is a problem with the protocols I showed you. How do you pick a Random Natural? How to fix this. Discuss
Modular Arithmetic

Arithmetic mod 14 works as follows:

1. The only numbers allowed are \( \{0, \ldots, 13\} \).
2. Addition and multiplication are wrap around:
   \[
   6 + 6 \equiv 12 \\
   6 + 7 \equiv 13 \\
   6 + 8 \equiv 0 \\
   5 \times 7 \equiv 35 \equiv 14 + 14 + 7 \equiv 7 \\
   5 \times 3 \equiv 15 \equiv 1.
   \]
3. Subtraction still works: \(-6\) is 8 since \(6 + 8 \equiv 0\).
4. Division sometimes works.
Modular Arithmetic

Arithmetic mod 14 works as follows:

1. The only numbers allowed are \{0, \ldots, 13\}.
2. Addition and multiplication are wrap around:
   \[
   \begin{align*}
   6 + 6 & \equiv 12 \\
   6 + 7 & \equiv 13 \\
   6 + 8 & \equiv 0 \\
   5 \times 7 & \equiv 35 \equiv 14 + 14 + 7 \equiv 7 \\
   5 \times 3 & \equiv 15 \equiv 1.
   \end{align*}
   \]
3. Subtraction still works: \(-6\) is 8 since \(6 + 8 \equiv 0\).
4. Division sometimes works.
   \(1/5\) is 3 since \(3 \times 5 \equiv 1\).
Modular Arithmetic

Arithmetic mod 14 works as follows:

1. The only numbers allowed are \{0, \ldots, 13\}.
2. Addition and multiplication are wrap around:
   \[
   \begin{align*}
   6 + 6 & \equiv 12 \\
   6 + 7 & \equiv 13 \\
   6 + 8 & \equiv 0 \\
   5 \times 7 & \equiv 35 \equiv 14 + 14 + 7 \equiv 7 \\
   5 \times 3 & \equiv 15 \equiv 1.
   \end{align*}
   \]
3. Subtraction still works: \(-6\) is 8 since \(6 + 8 \equiv 0\).
4. Division sometimes works.
   \[
   \begin{align*}
   1/5 & \text{ is 3 since } 3 \times 5 \equiv 1. \\
   1/2 & \text{ does not exist.}
   \end{align*}
   \]
If you work mod a Prime... 

If you work mod a prime
If you work mod a Prime...

1. Every element of \{1, \ldots, p - 1\} has an inverse.
If you work mod a Prime...

If you work mod a prime

1. Every elements of \( \{1, \ldots, p - 1\} \) has an inverse.
2. 2 points determine a line.
If you work mod a Prime... 

If you work mod a prime 

1. Every elements of \( \{1, \ldots, p - 1\} \) has an inverse. 
2. 2 points determine a line. 
3. \( t \) points determine a \( t - 1 \)-degree-curve.
Real Solution to \((t, m)\)-Secret Sharing

1. Zelda has a secret \(s \in \{0, \ldots, p-1\}\) where \(p\) is a prime. All arithmetic in this protocol is mod \(p\).

2. Zelda picks random \(r_1, \ldots, r_{t-1} \in \{0, \ldots, p-1\}\). Let \(f(x) = r_{t-1}x^{t-1} + \cdots + r_1x + s\).

3. Zelda gives \(A_1f(1), A_2f(2), \ldots, A_pf(m)\). If any \(t\) get together they have \(t\) points on a \(t-1\) degree curve \(f\), so they can find the equation for \(f\), and hence \(s\). If any \(t-1\) get together they don't learn anything about \(s\).
Real Solution to \((t, m)\)-Secret Sharing

1. Zelda has a \textbf{secret} \(s \in \{0, \ldots, p - 1\}\) where \(p\) is a prime. \textbf{All} arithmetic in this protocol is mod \(p\).
Real Solution to \((t, m)\)-Secret Sharing

1. Zelda has a **secret** \(s \in \{0, \ldots, p - 1\}\) where \(p\) is a prime. **All** arithmetic in this protocol is mod \(p\).

2. Zelda picks random \(r_1, \ldots, r_{t - 1} \in \{0, \ldots, p - 1\}\). Let \(f\) be

\[
f(x) = r_{t-1} x^{t-1} + \cdots + r_1 x + s.
\]
1. Zelda has a secret $s \in \{0, \ldots, p - 1\}$ where $p$ is a prime. All arithmetic in this protocol is mod $p$.

2. Zelda picks random $r_1, \ldots, r_{t-1} \in \{0, \ldots, p - 1\}$. Let $f$ be

$$f(x) = r_{t-1}x^{t-1} + \cdots + r_1x + s.$$ 

3. Zelda gives $A_1 \ f(1), \ A_2 \ f(2), \ldots, A_m \ f(m)$. 
1. Zelda has a **secret** $s \in \{0, \ldots, p - 1\}$ where $p$ is a prime. **All** arithmetic in this protocol is mod $p$.

2. Zelda picks random $r_1, \ldots, r_{t-1} \in \{0, \ldots, p - 1\}$. Let $f$ be

   \[ f(x) = r_{t-1} x^{t-1} + \cdots + r_1 x + s. \]

3. Zelda gives $A_1 f(1), A_2 f(2), \ldots, A_m f(m)$.

   If any $t$ get together they have $t$ points on a $t - 1$-degree–curve $f$, so they can find the equation for $f$, and hence $s$. 

**Real Solution to** $(t, m)$-Secret Sharing
Real Solution to \((t, m)\)-Secret Sharing

1. Zelda has a **secret** \(s \in \{0, \ldots, p - 1\}\) where \(p\) is a prime. **All** arithmetic in this protocol is mod \(p\).

2. Zelda picks random \(r_1, \ldots, r_{t-1} \in \{0, \ldots, p - 1\}\). Let \(f\) be

\[
f(x) = r_{t-1}x^{t-1} + \cdots + r_1x + s.
\]

3. Zelda gives \(A_1 f(1), A_2 f(2), \ldots, A_m f(m)\).

If any \(t\) get together they have \(t\) points on a \((t - 1)\)-degree–curve \(f\), so they can find the equation for \(f\), and hence \(s\). If any \(t - 1\) get together they don’t learn **anything** about \(s\).
Applications

Rumor Secret Sharing is used for the Russian Nuclear Codes. There are three people (one is Putin) and if two of them agree to launch, they can launch.
Applications

**Rumor** Secret Sharing is used for the Russian Nuclear Codes. There are three people (one is Putin) and if two of them agree to launch, they can launch.

**Fact** For people signing a contract long distance, secret sharing is used as a building block in the protocol.
Rumor Secret Sharing is used for the Russian Nuclear Codes. There are three people (one is Putin) and if two of them agree to launch, they can launch.

Fact For people signing a contract long distance, secret sharing is used as a building block in the protocol.

Fact Secret Sharing is a building block for other protocols including voting-in-secret and secure computation.