Uniqueness of Solutions

Public Key Cryptography

Prof Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2013 – Crupto PK 1/4
Recorded: October 8, 2013

Solving an equation

Lemma

If a has a multiplicative inverse $a^{-1} \in \mathbb{Z}_n$, then the equation

$$a \cdot x = b \quad \text{in } \mathbb{Z}_n$$

has the unique solution

$$x = a^{-1} \cdot b.$$

We proved the solution, but not uniqueness.

HØGSKOLEN I ÅLESUND
Aalesund University College

Problem

Exercise

Prove that the solution in the lemma is indeed unique.

Exercise

Prove that if a has an inverse a^{-1}, then it is unique.

HØGSKOLEN I ÅLESUND
Aalesund University College

Uniqueness of inverses

Theorem

If an element in $\mathbb{Z}_n$ has an inverse, then it has exactly one inverse.

HØGSKOLEN I ÅLESUND
Aalesund University College

Uniqueness of Solution

Formalisation

The solution $x = a^{-1}b$ to the equation $ax = b$ in $\mathbb{Z}_n$ is unique.

1. We formalise
   - $\forall x \in \mathbb{Z}_n, ax = b \Rightarrow x = a^{-1}b$
2. Universal generalistion and indirect proof
   - Let x be any $x \in \mathbb{Z}_n$
   - Assume $ax = b$
   - Then we can multiply by a^{-1}
   - Thus $a = a^{-1}x$
3. This is valid for any x, so the claim holds

HØGSKOLEN I ÅLESUND
Aalesund University College

Uniqueness of Solution

Formalisation

The solution $x = a^{-1}b$ to the equation $ax = b$ in $\mathbb{Z}_n$ is unique.

1. We formalise
   - $\forall x \in \mathbb{Z}_n, ax = b \Rightarrow x = a^{-1}b$
2. Universal generalistion and indirect proof
   - Let x be any $x \in \mathbb{Z}_n$
   - Assume $ax = b$
   - Then we can multiply by a^{-1}
   - Thus $a = a^{-1}x$
3. This is valid for any x, so the claim holds

HØGSKOLEN I ÅLESUND
Aalesund University College

Uniqueness of Solution

Formalisation

The solution $x = a^{-1}b$ to the equation $ax = b$ in $\mathbb{Z}_n$ is unique.

1. We formalise
   - $\forall x \in \mathbb{Z}_n, ax = b \Rightarrow x = a^{-1}b$
2. Universal generalistion and indirect proof
   - Let x be any $x \in \mathbb{Z}_n$
   - Assume $ax = b$
   - Then we can multiply by a^{-1}
   - Thus $a = a^{-1}x$
3. This is valid for any x, so the claim holds

HØGSKOLEN I ÅLESUND
Aalesund University College

Summary

- Inverses is the key to solving equations
- Solutions to first order equations are unique
- Inverses are unique