Modular and Non-modular Equations

Public Key Cryptography

Prof Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2013 – Crypto PK 2/1
Recorded: 8th October 2013

Motivation

Problem

Given an element $a \in \mathbb{Z}_n$, how do we find a^{-1}?

- Necessary to solve equations
- Necessary to derive RSA keys
- Non-trivial — It will take some videos to answer

HØGSKOLEN I ÅLESUND
Aalesund University College

Rewriting equations

Modular equation

$$ax = 1 \quad \text{in } \mathbb{Z}_n$$

Congruence

$$ax \equiv 1 \pmod{n}$$

Normal equation

$$\exists y \in \mathbb{Z}, ax + ny = 1$$

I.e. we solve $ax + ny = 1$ for x and y

Any modular equation can be thought of in either of these three ways.

An equation

The multiplicative inverse

- Equivalent problems
  1. Solve $ax = 1$ for x in $\mathbb{Z}_n$
  2. Solve $ax + ny = 1$ for x and y in $\mathbb{Z}$

Lemma

The equation $ax = 1$ has a solution in $\mathbb{Z}_n$ if and only if there exist integers x and y such that

$$ax + ny = 1 \quad \text{in } \mathbb{Z}.$$

Recall, unique solution if a^{-1} exists, and no solution otherwise.

HØGSKOLEN I ÅLESUND
Aalesund University College

The multiplicative inverse

Theorem

A number $a \in \mathbb{Z}_n$ has a multiplicative inverse if and only if there are integers x and y such that $ax + ny = 1$ in $\mathbb{Z}$.

- Proof.
  - We knew that a^{-1} if and only if $ax = 1$ has a solution in $\mathbb{Z}_n$
  - We found that $ax = 1$ has a solution in $\mathbb{Z}_n$ if and only if $ax + ny = 1$ has a solution in $\mathbb{Z}$
  - The theorem follow.

Corollary

Using the solution above, $a^{-1} = x \mod n$.

Summary

- Three equivalent problems
  1. Solve $ax = 1$ for x in $\mathbb{Z}_n$
  2. Solve $ax + ny = 1$ for x and y in $\mathbb{Z}$
  3. Find the inverse of a in $\mathbb{Z}_n$

HØGSKOLEN I ÅLESUND
Aalesund University College