Extended Euclid's Algorithm

Multiplicative Inverses

Prof Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2013 – Crupto PK 3/2
Recorded: October 9, 2013

Multiplicative inverses

$$1 = a \cdot x + n \cdot y$$

- If there is a solution (x, y), then
  1. a has an inverse in $\mathbb{Z}_n$
  2. $\mathrm{hcf}(a, n) = 1$
- The converse is also true
- We have $a^{-1} = x \mod n$
- More generally, if $d = \mathrm{hcf}(a, n)$, then we can solve

$$d = a \cdot x + n \cdot y$$

HØGSKOLEN I ÅLESUND
Aalesund University College

Multiplicative inverses

$$1 = a \cdot x + n \cdot y$$

- If there is a solution (x, y), then
  1. a has an inverse in $\mathbb{Z}_n$
  2. $\mathrm{hcf}(a, n) = 1$
- The converse is also true
- We have $a^{-1} = x \mod n$
- More generally, if $d = \mathrm{hcf}(a, n)$, then we can solve

$$d = a \cdot x + n \cdot y$$

HØGSKOLEN I ÅLESUND
Aalesund University College

The process

$$n = aq_1 + r_1 \tag{1}$$
$$a = r_1 q_2 + r_2 \tag{2}$$
$$r_1 = r_2 q_3 + r_3 \tag{3}$$
$$r_2 = r_3 q_4 + r_4 \tag{4}$$
$$\vdots \tag{5}$$
$$r_{m-2} = r_{m-1} q_m + r_m \tag{6}$$
$$r_{m-1} = r_m q_{m+1} + 0 \tag{7}$$

HØGSKOLEN I ÅLESUND
Aalesund University College

Numeric Example

Exercise

What is the inverse of 12 mod 55*?*

Numeric Example

$$x = 23 \quad y = -5$$

Exercise

Exercise

Find the inverse of $28 \mod 81$.