# 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

$$\boxed{1 = a \cdot x + n \cdot y}$$

- 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 $\boxed{a^{-1} = x \mod n}$
- More generally, if $d = \mathrm{hcf}(a, n)$, then we can solve

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

# 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

$$\boxed{d = a \cdot x + n \cdot y}$$

HØGSKOLEN I ÅLESUND
Aalesund University College

# The process

$\boxed{\begin{aligned} x' &= y \\ y' &= x - q\,y \end{aligned}}$

$HCF(a, n)$

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

$$n = aq_1 + r_1 \quad (1)$$
$$a = r_1 q_2 + r_2 \quad (2)$$
$$r_1 = r_2 q_3 + r_3 \quad (3)$$
$$r_2 = r_3 q_4 + r_4 \quad (4)$$
$$\vdots \quad (5)$$

$r_{m-3} = r_{m-2} q_{m-1} + r_{m-1}$

$r_{m-1} = 1 \cdot r_{m-3} + (-q_{m-1}) r_{m-2}$

$$r_{m-2} = r_{m-1} q_m + r_m \quad (6)$$

$r_m = \underbrace{1}_{x} \cdot r_{m-2} + \underbrace{(-q_m)}_{y} r_{m-1}$

$$r_{m-1} = r_m q_{m+1} + 0 \quad (7)$$

$r_m = 1 \cdot r_{m-2} + [-q_m][r_{m-3} + (-q_{m-1}) r_{m-2}]$

$\underbrace{[-q_m]}_{x'} r_{m-3} + \underbrace{[1 - q_{m-1}(-q_m)]}_{y} r_{m-2}$



HØGSKOLEN I ÅLESUND
Aalesund University College

# Numeric Example

## Exercise

*What is the inverse of* 12 mod 55?

$$1 = a \cdot \overset{23}{x} + n \cdot \overset{-5}{y}$$

HCF(12, 55)

| | | $q$ | |
|---|---|---|---|
| $55$ | $= 12 \cdot$ | $4$ | $+ 7$ |
| $12$ | $= 7 \cdot$ | $1$ | $+ 5$ |
| $7$ | $= 5 \cdot$ | $1$ | $+ 2$ |
| $5$ | $= 2 \cdot$ | $2$ | $+ 1$ |
| $2$ | $= 1 \cdot$ | $2$ | $+ 0$ |

| | $x$ | | $y$ |
|---|---|---|---|
| | $-5$ | | $3 - 4 \cdot (-5) = 23$ |
| | $3$ | | $-2 - 1 \cdot 3 = -5$ |
| | $-2$ | | $1 - 1 \cdot (-2) = 3$ |
| $1 =$ | $1 \cdot 5$ | $+$ | $(-2) \cdot 2$ |

# Numeric Example

$a = 12$

$n = 55$

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

$x \cdot a + y \cdot n$

$23 \cdot 12 + (-5) \cdot 55$

$276 - 275 = 1$

$$\boxed{\begin{array}{l} 23 \cdot 12 = 276 \\ 276 \bmod 55 = 1 \end{array}}$$

$a^{-1} = 23$

# Exercise

**Exercise**

*Find the inverse of* $28 \mod 81$.