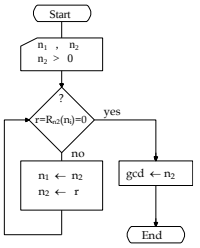
# Introduction to Cryptology

**Tutorial-1**
**Mathematical Background: Remainder System, gcd**

*07.03.2023, v35*



## Eucledian gcd Algorithm




**Example:**

**Rest of dividing $n_1$ by $n_2$**

| n1 | n2 | r |
|---|---|---|
| 132 | 108 | 24 |
| 108 | 24 | 12 |
| 24 | 12 | 0 |

gcd

Complexity < $\log_2 n + 1$ operations
$n = \text{Max}[n_1, n_2]$



## Extended gcd Algorithm and the Multiplicative Inverse

**$\gcd(n_1, n_2) = a \cdot n_1 + b \cdot n_2$**

Question: Find the multiplicative inverse of $n_2$ modulo $n_1$

Solution: Compute $\gcd(n_1,n_2) = a \cdot n_1 + b \cdot n_2 \stackrel{?}{=} 1$
If gcd = 1, then the inverse is **b**

| | | | | | $a_1-qa_2$ | $b_1-qb_2$ | | | |
|---|---|---|---|---|---|---|---|---|---|
| $n_1$ | $n_2$ | $a_1$ | $b_1$ | $a_2$ | $b_2$ | | q | r | computation |
| .. | .. | 1 | 0 | 0 | 1 | | .. | .. | |
| .. | .. | .. | .. | .. | .. | | .. | .. | |
| .. | 1 | .. | … | … | … | | .. | .. | |

gcd

$\gcd(n_2,n_1)$ $= a \cdot n_1 + b \cdot n_2 = 1$
$R_{n1}\ (a \cdot n_1 + b \cdot n_2) = 1$
$R_{n1}\ (\ 0 \ + b \cdot n_2) = 1 \quad \Rightarrow b = n_2^{-1} \pmod{n_1}$



## Problem 1-1: Compute the following:

$R_{21}\ (45 \cdot 65 \cdot 220) =$
$R_{21}\ (45 + 65 - 220) =$
$R_{13}\ (12^5 - 28 \cdot 15^3) =$

## Solution 1-1:

$R_{21}\ (45 \cdot 65 \cdot 220) = R_{21}\ (3 \cdot 2 \cdot 10) = R_{21}\ (3 \cdot -1\ ) = -3 = -3 + 21 = \mathbf{18}$

$R_{21}\ (45 + 65 - 220) = R_{21}\ (3 + 2 - 10) = R_{21}\ (-5) = \mathbf{16}$

$R_{13}\ (12^5 - 28 \cdot 15^3) = R_{13}\ (-1^5 - 2 \cdot 2^3) = R_{13}\ (-1 - 2 \times 8)$
$= R_{13}\ (-1 - 16) = R_{13}\ (-1 - 3) = R_{13}\ (-4) = \mathbf{9}$



## Problem 1-2 & Solution 1-2:

Find gcd (245,295)

| n1 | n2 | r |
|---|---|---|
| 295 | 245 | 50 |
| 245 | 50 | 45 |
| 50 | 45 | 5 |
| 45 | 5 | 0 |

**Gcd (295,245) = 5**

Find gcd (624,336)

| n1 | n2 | r |
|---|---|---|
| 624 | 336 | 288 |
| 336 | 288 | 48 |
| 288 | 48 | 0 |

**gcd (624,336) = 48**

Find gcd (142,35)

| n1 | n2 | r |
|---|---|---|
| 142 | 35 | 2 |
| 35 | 2 | 1 |
| 2 | 1 | 0 |

**gcd (142,35) = 1 (relatively prime)**

Find gcd (3234,3206)

| n1 | n2 | r |
|---|---|---|
| 3234 | 3206 | 28 |
| 3206 | 28 | 14 |
| 28 | 14 | 0 |

**gcd (3234,3206) = 14**



## Problem 1-3: Find the multiplicative inverse of **26** modulo **31**

**Solution 1-3:** Compute $\gcd(31, 26) = a \cdot 31 + b \cdot 26 \stackrel{?}{=} 1$
if gcd = 1, then the inverse is **b**

| | | | | | $a_1-qa_2$ | $b_1-qb_2$ | | | |
|---|---|---|---|---|---|---|---|---|---|
| $n_1$ | $n_2$ | $a_1$ | $b_1$ | $a_2$ | $b_2$ | | q | r | computation |
| 31 | 26 | 1 | 0 | 0 | 1 | 1 | 5 | 31/26 = 1 + 5/26 |
| 26 | 5 | 0 | 1 | 1 | 0-1*1 = -1 | 5 | 1 | 26/5 = 5+1/5 |
| 5 | 1 | 1 | -1 | 0-5*1 = -5 | 1-5*-1 = 6 | 5 | 0 | 5/1 = 5+ 0/1 |

gcd

$\gcd(31,26)$ $= a \cdot 31 + b \cdot 26$
$= -5 \cdot 31 + 6 \cdot 26 = 1$, Check! $-155 + 156 = 1$

Operating modulo 31: $R_{31}(-5 \cdot 31 + 6 \cdot 26) = R_{31}(1)$
$\Rightarrow R_{31}(\ 0 \ + 6 \cdot 26) = 1$
$\Rightarrow$ The inverse of 26 modulo 31 is $\boxed{26^{-1} = 6}$ **(mod 31 )**
**Check** $6 \cdot 26 = 156 = 1 \mod 31$ q.e.d

**Problem 1-4:** Find the multiplicative inverse of **18** modulo **23**

**Solution 1-4:** Compute gcd (23, 9) = a • 23 + b • 9 $\stackrel{?}{=}$ 1
if gcd = 1, then the inverse is **b**

$b_1$-$qb_2$

| $n_1$ | $n_2$ | | $b_1$ | $b_2$ | q | r | computation |
|---|---|---|---|---|---|---|---|
| 23 | 9 | | 0 | 1 | 2 | 5 | 23/9 = 2 + 5/23 |
| 9 | 5 | | 1 | 0-2x1 = -2 | 1 | 4 | 9/5 = 1 + 4/9 |
| 5 | 4 | | -2 | 1-1x-2 = 3 | 1 | 1 | 5/4 = 1 + 1/4 |
| 4 | 1 | | 3 | -2-1x3 = -5 | 4 | 0 | |
| | | | | | | | |

gcd

-5 = -5+23 = 18

**9 • 18 mod 23 ≡ 162 ≡ 1**

**=> $9^{-1}$ ≡ 18 (mod 23)**



## General Extended gcd Solution as Excel Sheet:

**Solution:** Compute gcd (23, 17) = a • 23 + b • 17 $\stackrel{?}{=}$ 1
if gcd = 1, then the inverse is **b**

| m | u | a1 | a2 | b1 | b2 | q | r | INVERSE VALUE = B2 | | GCD | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 23 | 17 | 1 | 0 | 0 | 1 | 1 | 6 | | | | |
| 17 | 6 | 0 | 1 | 1 | -1 | 2 | 5 | | | | |
| 6 | 5 | 1 | -2 | -1 | 3 | 1 | 1 | | | | |
| 5 | 1 | -2 | 3 | 3 | -4 | 5 | 0 | NVERSE= | -4 | GCD= | 1 |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

Check: 17 • -4 = -68 = 1 mod 23
or 17 • (23 – 4) = 17 • 19 = 323 = 1 mod 23