

Foundation of Cryptography

Session 18

Date: 15 March 2021

Dr. V. K. Pachghare

Number Theory

- **Extended Euclidean Algorithm**
- **Chinese Remainder Theorem**

Extended Euclidean Algorithm

- Get not only GCD but x and y such that

$$ax + by = d = \text{GCD}(a, b)$$

- follow sequence of divisions for GCD but at each step keep track of x and y :

$$r = ax + by$$

- at the end find GCD value and also x and y
- if $\text{GCD}(a, b) = 1 = ax + by$ then x is inverse of

$$a \bmod b \text{ (or mod } y)$$

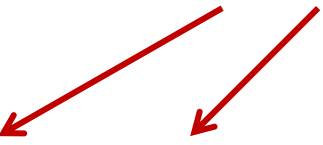
- We can use it to find the multiplicative inverse

**Find the multiplicative inverse of
3 mod 20**

$$20 = 6 \times 3 + 2$$

3 mod 20

$$20 = 6 \times 3 + 2$$

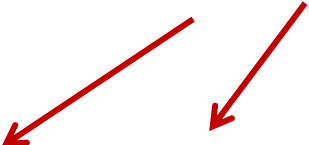
$$3 = 1 \times 2 + 1$$


3 mod 20

$$20 = 6 \times 3 + 2$$

$$3 = 1 \times 2 + 1$$

$$2 = 2 \times 1 + 0$$



3 mod 20

$$20 = 6 \times 3 + 2$$

$$3 = 1 \times 2 + 1$$

$$2 = 2 \times 1 + 0$$

$$2 = 20 - 6 \times 3$$

$$1 = 3 - 1 \times 2$$

3 mod 20

$$20 = 6 \times 3 + 2$$

$$3 = 1 \times 2 + 1$$

$$2 = 2 \times 1 + 0$$

$$1 = 3 - 1 \times 2$$

$$2 = 20 - 6 \times 3$$

$$1 = 3 - 1 \times 2$$

3 mod 20

$$20 = 6 \times 3 + 2$$

$$3 = 1 \times 2 + 1$$

$$2 = 2 \times 1 + 0$$

$$\mathbf{2} = 20 - 6 \times 3$$

$$\mathbf{1} = 3 - 1 \times 2$$

$$\mathbf{1} = 3 - 1 \times \mathbf{2}$$

$$1 = 3 - [20 - 3(6)] (1)$$

3 mod 20

$$20 = 6 \times 3 + 2$$

$$3 = 1 \times 2 + 1$$

$$2 = 2 \times 1 + 0$$

$$\mathbf{2} = 20 - 6 \times 3$$

$$\mathbf{1} = 3 - 1 \times 2$$

$$\mathbf{1} = 3 - 1 \times \mathbf{2}$$

$$1 = 3 - [20 - 3(6)] (1)$$

$$1 = 3 - 20(1) + 3(6)$$

3 mod 20

$$20 = 6 \times 3 + 2$$

$$3 = 1 \times 2 + 1$$

$$2 = 2 \times 1 + 0$$

$$\mathbf{2} = \mathbf{20} - \mathbf{6} \times \mathbf{3}$$

$$\mathbf{1} = \mathbf{3} - \mathbf{1} \times \mathbf{2}$$

$$\mathbf{1} = \mathbf{3} - \mathbf{1} \times \mathbf{2}$$

$$1 = 3 - [20 - 3(6)] (1)$$

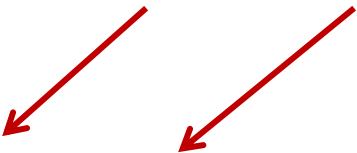
$$1 = 3 - 20(1) + 3(6)$$

$$1 = 3(\mathbf{7}) + 20(-1)$$

7 is the multiplicative inverse of 3 mod 20

9 mod 26

$$26 = 9 * 2 + 8$$


$$9 = 8(1) + 1$$

$9 \bmod 26$

$$26 = 9 * 2 + 8$$

$$8 = 26 - 9(2)$$

$$9 = 8(1) + 1$$

$$1 = 9 - 8(1)$$

9 mod 26

$$26 = 9 * 2 + 8$$

$$9 = 8(1) + 1$$

$$1 = 9 - 8(1)$$

$$8 = 26 - 9(2)$$

$$1 = 9 - 8(1)$$

9 mod 26

$$26 = 9 * 2 + 8$$

$$9 = 8(1) + 1$$

$$8 = 26 - 9(2)$$

$$1 = 9 - 8(1)$$

$$1 = 9 - 8(1)$$

$$1 = 9 - [26 - 9(2)](1)$$

9 mod 26

$$26 = 9 * 2 + 8$$

$$8 = 26 - 9(2)$$

$$9 = 8(1) + 1$$

$$1 = 9 - 8(1)$$

$$1 = 9 - 8(1)$$

$$1 = 9 - [26 - 9(2)](1)$$

$$1 = 9(3) + 26(-1)$$

Multiplicative inverse of 9 mod 26 is 3

Find integers p and q such that $2322p + 654q = 6$ and also find the $\text{GCD}(2322, 654)$.

$$2322 = 654(3) + 360$$

$$654 = 360(1) + 294$$

$$360 = 294(1) + 66$$

$$294 = 66(4) + 30$$

$$66 = 30(2) + 6(\text{GCD})$$

$$30 = 6(5) + 0$$

$$360 = 2322 - 654(3)$$

$$294 = 654 - 360(1)$$

$$66 = 360 - 294(1)$$

$$30 = 294 - 66(4)$$

$$6 = 66 - 30(2)$$

$$6 = 66 - 30(2)$$

$$6 = 66 - [294 - 66(4)](2)$$

$$6 = 66(9) - 294(2)$$

$$6 = [360 - 294(1)](9) - 294(2)$$

$$6 = 360(9) - 294(11)$$

$$6 = 360(9) - [654 - 360(1)](11)$$

$$6 = 360(20) - 654(11)$$

$$6 = [2322 - 654(3)](20) - 654(11)$$

$$6 = 2322(20) - 654(71)$$

Therefore, the values of $p = 20$ and $q = -71$ and $\text{GCD} = 6$.

Find integers p , and q such that $51p + 36q = 3$. Also find the GCD $(51, 36)$.

Find integers p , and q such that $51p + 36q = 3$. Also find the GCD (51, 36).

- The identity states for 2 numbers x and y with Greatest Common Divisor g , an equation exists that says $g = xp + yq$

Find integers p , and q such that $51p + 36q = 3$. Also find the GCD $(51, 36)$.

- The identity states for 2 numbers x and y with Greatest Common Divisor g , an equation exists that says $g = xp + yq$

$$51 = 36(1) + 15$$

Find integers p , and q such that $51p + 36q = 3$. Also find the GCD (51, 36).

- The identity states for 2 numbers x and y with Greatest Common Divisor g , an equation exists that says $g = xp + yq$

$$51 = 36(1) + 15$$

$$36 = 15(2) + 6$$

Find integers p , and q such that $51p + 36q = 3$. Also find the GCD (51, 36).

- The identity states for 2 numbers x and y with Greatest Common Divisor g , an equation exists that says $g = xp + yq$

$$51 = 36(1) + 15$$

$$36 = 15(2) + 6$$

$$15 = 6(2) + \mathbf{3 \text{ (GCD)}}$$

Find integers p , and q such that $51p + 36q = 3$. Also find the GCD (51, 36).

- The identity states for 2 numbers x and y with Greatest Common Divisor g , an equation exists that says $g = xp + yq$

$$51 = 36(1) + 15$$

$$36 = 15(2) + 6$$

$$15 = 6(2) + \mathbf{3 \text{ (GCD)}}$$

$$6 = 3(2) + 0$$

Find integers p , and q such that $51p + 36q = 3$. Also find the GCD $(51, 36)$.

- The identity states for 2 numbers x and y with Greatest Common Divisor g , an equation exists that says $g = xp + yq$

$51 = 36(1) + 15$	$15 = 51 - 36(1)$
$36 = 15(2) + 6$	$6 = 36 - 15(2)$
$15 = 6(2) + 3$ (GCD)	$3 = 15 - 6(2)$
$6 = 3(2) + 0$	

$$3 = 15 - 6(2)$$

$$15 = 51 - 36(1)$$

$$6 = 36 - 15(2)$$

$$3 = 15 - 6(2)$$

$$3 = 15 - 6(2)$$

$$3 = 15 - [36 - 15(2)](2)$$

$$15 = 51 - 36(1)$$

$$6 = 36 - 15(2)$$

$$3 = 15 - 6(2)$$

$$3 = 15 - 6(2)$$

$$3 = 15 - [36 - 15(2)](2)$$

$$3 = 15(5) - 36(2)$$

$$15 = 51 - 36(1)$$

$$6 = 36 - 15(2)$$

$$3 = 15 - 6(2)$$

$$3 = 15 - 6(2)$$

$$3 = 15 - [36 - 15(2)](2)$$

$$3 = 15(5) - 36(2)$$

$$3 = [51 - 36(1)](5) - 36(2)$$

$$15 = 51 - 36(1)$$

$$6 = 36 - 15(2)$$

$$3 = 15 - 6(2)$$

$$3 = 15 - 6(2)$$

$$3 = 15 - [36 - 15(2)](2)$$

$$3 = 15(5) - 36(2)$$

$$3 = [51 - 36(1)](5) - 36(2)$$

$$3 = 51(5) - 36(5) - 36(2)$$

$$15 = 51 - 36(1)$$

$$6 = 36 - 15(2)$$

$$3 = 15 - 6(2)$$

$$3 = 15 - 6(2)$$

$$3 = 15 - [36 - 15(2)](2)$$

$$3 = 15(5) - 36(2)$$

$$3 = [51 - 36(1)](5) - 36(2)$$

$$3 = 51(5) - 36(5) - 36(2)$$

$$3 = 51(5) - 36(7)$$

$$15 = 51 - 36(1)$$

$$6 = 36 - 15(2)$$

$$3 = 15 - 6(2)$$

$$3 = 15 - 6(2)$$

$$3 = 15 - [36 - 15(2)](2)$$

$$3 = 15(5) - 36(2)$$

$$3 = [51 - 36(1)](5) - 36(2)$$

$$3 = 51(5) - 36(5) - 36(2)$$

$$3 = 51(5) - 36(7)$$

$$3 = 51(5) + 36(-7)$$

$$15 = 51 - 36(1)$$

$$6 = 36 - 15(2)$$

$$3 = 15 - 6(2)$$

$$3 = 15 - 6(2)$$

$$3 = 15 - [36 - 15(2)](2)$$

$$3 = 15(5) - 36(2)$$

$$3 = [51 - 36(1)](5) - 36(2)$$

$$3 = 51(5) - 36(5) - 36(2)$$

$$3 = 51(5) - 36(7)$$

$$3 = 51(5) + 36(-7)$$

Therefore, the values of $p = 5$ and $q = -7$ and $\text{GCD} = 3$.