

# Chapter 28: Euclidean Algorithm

---

- Euclidean Algorithm
- Extended Euclidean Algorithm
- Solving  $ax \bmod n = 1$
- Solving  $ax \bmod n = b$

# Overview

---

- Solving modular equations arises in cryptography
- Euclidean Algorithm
- From Euclid to solving  $ax \bmod n = 1$
- From  $ax \bmod n = 1$  to solving  $ax \bmod n = b$

# Euclidean Algorithm

---

- Given positive integers  $a$  and  $b$ , find their greatest common divisor
- Idea
  - if  $x$  is the greatest common divisor of  $a$  and  $b$ , then  $x$  divides  $r = a - b$
  - reduces problem to finding largest  $x$  that divides  $r$  and  $b$
  - iterate

# Example 1

---

- Take  $a = 15, b = 12$

$a$	$b$	$q$	$r$	
15	12	1	3	$q = 15/12 = 1$
				$r = 15 - 1 \times 12$
12	3	4	0	$q = 12/3 = 4$
				$r = 12 - 4 \times 3$

- so  $\gcd(15, 12) = 3$ 
  - The  $b$  for which  $r$  is 0

# Example 2

---

- Take  $a = 35731$ ,  $b = 25689$

$a$	$b$	$q$	$r$	
35731	24689	1	11042	$q = 35731/24689 = 1$ $r = 35731 - 1 \times 24689$
24689	11042	2	2,605	$q = 24689/11042 = 2$ $r = 24689 - 2 \times 11042$
11042	2605	4	622	$q = 11042/2605 = 4$ $r = 11042 - 4 \times 2605$
2605	622	4	117	$q = 2605/622 = 4$ ; $r = 2605 - 4 \times 622$
622	117	5	37	$q = 622/117 = 5$ ; $r = 622 - 5 \times 117$
117	37	3	6	$q = 117/37 = 3$ ; $r = 117 - 3 \times 37$
37	6	6	1	$q = 37/6 = 6$ ; $r = 37 - 6 \times 6$
6	1	6	0	$q = 6/1 = 6$ ; $r = 6 - 6 \times 1$

# Pseudocode

---

```
/* find gcd of a and b */  
rprev := r := 1;  
while r <> 0 do begin  
    rprev := r;  
    r := a mod b;  
    write 'a = ', a, 'b =', b, 'q = ', a div b,  
        'r = ', r, endlne;  
    a := b;  
    b := r;  
end;  
gcd := rprev;
```

# Extended Euclidean Algorithm

---

- Find two integers  $x$  and  $y$  such that

$$xa + yb = 1$$

# Example 1

---

- Find  $x$  and  $y$  such that  $51x + 100y = 1$

$u$	$x$	$y$	$q$	
100	0	1		
51	1	0	$100/51 = 1$	
49	-1	1	$51/49 = 1$	$u = 51 - 1 \times 49; x = 0 - 1 \times 1; y = 1 - 1 \times 0$
2	2	-1	$49/2 = 24$	$u = 51 - 1 \times 49; x = 1 - 1 \times (-1); y = 0 - 1 \times 1$
1	-49	25	$2/1 = 2$	$u = 49 - 24 \times 2; x = -1 - 24 \times 2; y = 1 - 24 \times (-1)$
0	100	-51		

- So,  $51 \times (-49) + 100 \times 25 = 1$ 
  - This is  $-2499 + 2500 = 1$



# Example 2

- Find  $x$  and  $y$  such that  $24689x + 35731y = 1$

$u$	$x$	$y$	$q$
35731	0	1	
24689	1	0	$35731/24689 = 1$
11042	-1	1	$24689/11042 = 2$ $u = 35731 - 1 \times 24689$ ; $x = 0 - 1 \times 1$ ; $y = 1 - 1 \times 0$
2605	3	-2	$11042/2,605 = 4$ $u = 24689 - 2 \times 11042$ ; $x = 1 - 2 \times (-1)$ ; $y = 0 - 2 \times 1$
622	-13	9	$2605/622 = 4$ $u = 11042 - 4 \times 2605$ ; $x = -1 - 4 \times 3$ ; $y = 1 - 4 \times (-2)$
117	55	-38	$622/117 = 5$ $u = 2605 - 4 \times 622$ ; $x = 3 - 4 \times (-13)$ ; $y = -2 - 4 \times 9$
37	-288	199	$117/37 = 3$ $u = 622 - 5 \times 117$ ; $x = -13 - 5 \times 55$ ; $y = -38 - 5 \times (-38)$
6	919	-635	$37/6 = 6$ $u = 117 - 3 \times 37$ ; $x = 55 - 3 \times (-288)$ ; $y = -38 - 3 \times 199$
1	-5802	4,009	$6/1 = 6$ $u = 37 - 6 \times 6$ ; $x = -288 - 6 \times 919$ ; $y = 199 - 6 \times (-635)$
0	$35731 - 24689$		$u = 6 - 6 \times 1$ ; $x = 919 - 6 \times (-5802)$ $y = -635 - 6 \times (4009)$

- So,  $24689 \times (-5802) + 35731 \times 4009 = 1$

# Pseudocode

---

```
/* find x and y such that ax + by = 1, for given a and b */
uprev := a; u := b;
xprev := 0; x := 1; yprev := 1; y := 0;
write 'u = ', uprev, ' x = ', xprev, ' y = ', yprev,  endl;
write 'u = ', u, ' x = ', x, ' y = ', y;
while u <> 0 do begin
    q := uprev div u;
    write 'q = ', q, endl;
    utmp := uprev - u * q; uprev := u; u := utmp;
    xtmp := xprev - x * q; xprev := x; x := xtmp;
    ytmp := yprev - y * q; yprev := y; y := ytmp;
    write 'u = ', u, ' x = ', x, ' y = ', y;
end;
write endl;
x := xprev; y := yprev;
```

# Solving $ax \bmod n = 1$

---

- If  $ax \bmod n = 1$  then choose  $k$  such that  $ax = 1 + kn$ , or  $ax - kn = 1$ . If  $b = -k$ , then  $ax + bn = 1$ .
- Use extended Euclidean algorithm to solve for  $a$

# Example

---

- Solve for  $x$ :  $51x \bmod 100 = 1$ 
  - Recall (from earlier example)  
 $51 \times (-49) + 100 \times 25 = 1$   
Then  $x = -49 \bmod 100 = 51$
- Solve for  $x$ :  $24689 \bmod 35731 = 1$ 
  - Recall (from earlier example)  
 $24689 \times (-5802) + 35731 \times 4009 = 1$   
Then  $x = -5802 \bmod 35731 = 29929$

# Solving $ax \bmod n = b$

---

- A fundamental law of modular arithmetic:

$$xy \bmod n = (x \bmod n)(y \bmod n) \bmod n$$

so if  $x$  solves  $ax \bmod n = 1$ , then as

$$b(ax \bmod n) = a(bx) \bmod n = b$$

$bx$  solves  $ax \bmod n = b$

# Example

---

- Solve for  $x$ :  $51x \bmod 100 = 10$ 
  - Recall (from earlier example) that if  $51y \bmod 100 = 1$ , then  $y = 51$ .  
Then  $x = 10 \times 51 \bmod 100 = 510 \bmod 100 = 10$
- Solve for  $x$ :  $24689 \bmod 35731 = 1753$ 
  - Recall (from earlier example) that if  $24689y \bmod 35731 = 1$ , then  $y = 29929$ .  
Then  $x = 1753 \times 29929 \bmod 35731 = 12429$