# CS557: Cryptography

## Elementary Number Theory-IV

S. Tripathy
IIT Patna

# Previous Class

- Elementary Number Theory
  - GCD
    - Euclidean Algorithm.
  - Group Theory
  - Modular arithmetic

# Multiplicative inverses in Zn

- Multiplicative inverse –
  - SOME, but not ALL elements have unique multiplicative inverse.
  - In Z9:
    - 3*0=0, 3*1=3, 3*2=6, 3*3=0, 3*4=3, 3*5=6, …, so 3 does not have a multiplicative inverse.
    - What about 4,

      4*2=8, 4*3=3, 4*7 =1 i.e, $4^{-1} = 7$

  - In Zn, x has a multiplicative inverse if and only if x and n are relatively prime.

    E.g., in $Z_9$, 3 (does not have) but 4 (has =7)
  - If gcd(x,m) = 1, as y varies, y*x takes on m distinct values, so for some value, y*x=1mod m.

# Fermat's theorem to compute Inverse

**Thm:** Let p be a prime

$$\forall\ x \in (Z_p)^* : \qquad x^{p-1} = 1 \text{ in } Z_p$$

So: $x \in (Z_p)^* \Rightarrow x \cdot x^{p-2} = 1 \Rightarrow x^{-1} = x^{p-2}$ in $Z_p$

Another way to compute inverses, but less efficient

Example: p=5. What is the inverse of 3 mod 5?

$3^4 = 81 = 1$ in $Z_5$

$3^3 = 27 \bmod 5 = 2$

- Extende
  - given p … s
    such t
  - Ex.: F

2011 Week - 49

$a = bq + r$

$8^{-1} \bmod 11$

$GCD(8, 11) = 1$

$11 = 8(1) + 3$

$8 = 3(2) + 2$

$3 = 2(1) + 1$

$2 = 1(2) + 0$

GCD = 1 Reminder = 0

$3 = 11 - 8(1)$

$2 = 8 - 3(2)$

$1 = 3 - 2(1)$

$GCD = 1 = 3 - 2(1)$

$= 3 - [8 - 3(2)](1)$

$= -8(1) + 3(3)$

$= 8(-1) + [11 - 8(1)](3)$

$= 11(3) + 8(-4)$

# Euclidean Algorithm

- an efficient way to find the GCD(a,b)
- uses theorem that:
  - `GCD(a,b) = GCD(b, a mod b)`
- Euclidean Algorithm to compute GCD(a,b) is:

```
EUCLID(a,b)
1. A = a; B = b
2. if B = 0 return  A = gcd(a, b)
3. R = A mod B
4. A = B
5. B = R
6. goto 2
```

# Finding Inverses

```
EXTENDED EUCLID(m, b)
1. (A1, A2, A3)=(1, 0, m);  (B1, B2, B3)=(0, 1, b)
2. if B3 = 0
   return A3 = gcd(m, b); no inverse
3. if B3 = 1 // B3 = gcd(m, b);
   return B2 = b^-1 mod m
4. Q = A3 div B3
5. (T1, T2, T3)=(A1 − Q B1, A2 − Q B2, A3 − Q B3)
6. (A1,A2,A3)=(B1,B2,B3);(B1, B2, B3)=(T1,T2, T3)
8. goto 2
```

| Q | A1 | A2 | A3 | B1 | B2 | B3 |
|---|---|---|---|---|---|---|
| — | 1 | 0 | 1759 | 0 | 1 | 550 |
| 3 | 0 | 1 | 550 | 1 | –3 | 109 |
| 5 | 1 | –3 | 109 | –5 | 16 | 5 |
| 21 | –5 | 16 | 5 | 106 | –339 | 4 |
| 1 | 106 | –339 | 4 | –111 | 355 | 1 |

Inverse of 550 mod 1759 = 355

# Application Examples

Ex: Find a s.t. $3a \equiv 1 \pmod 7$.

Sol: since $\gcd(3,7) = 1$. the inverse of 3 (mod 7) exists and can be computed by the Euclidean algorithm:

$7 = 3 \times 2 + 1 \Rightarrow 1 = 7 + 3\,(-2).\ \therefore\ 3\,(-2) \equiv 1 \pmod 7$

$\Rightarrow a = -2 + 7k$ for all $k \in Z$.

Sol: $-2$ is an inverse of 3 (mod 7).

EX: Find all solutions of $3x \equiv 4 \pmod 7$.

=> $x = 4\,(-2) + 7k$ where $k \in Z$ is a general solution of $x$.

# Fast Exponentiation

- Usual approach to compute $x^c$ is inefficient when c is large.
- Instead, represent c as bit string $b_{k-1} \ldots b_0$ and use the following algorithm:
- z = 1
- For i = k-1 downto 0 do

  $z = z^2 \bmod n$

  if bi= 1 then z = z * x mod n
- Endfor

- Complexity: (k+k=) 2k modular multiplication

# $30^{37} \pmod{77}$?

| i | b | z | |
|---|---|---|---|
| 5 | 1 | 30 | =1*1*30 mod 77 |
| 4 | 0 | 53 | =30*30 mod 77 |
| 3 | 0 | 37 | =53*53 mod 77 |
| 2 | 1 | 29 | =37*37*30 mod 77 |
| 1 | 0 | 71 | =29*29 mod 77 |
| 0 | 1 | 2 | =71*71*30 mod 77 |

# Thanks