CS557: Cryptography

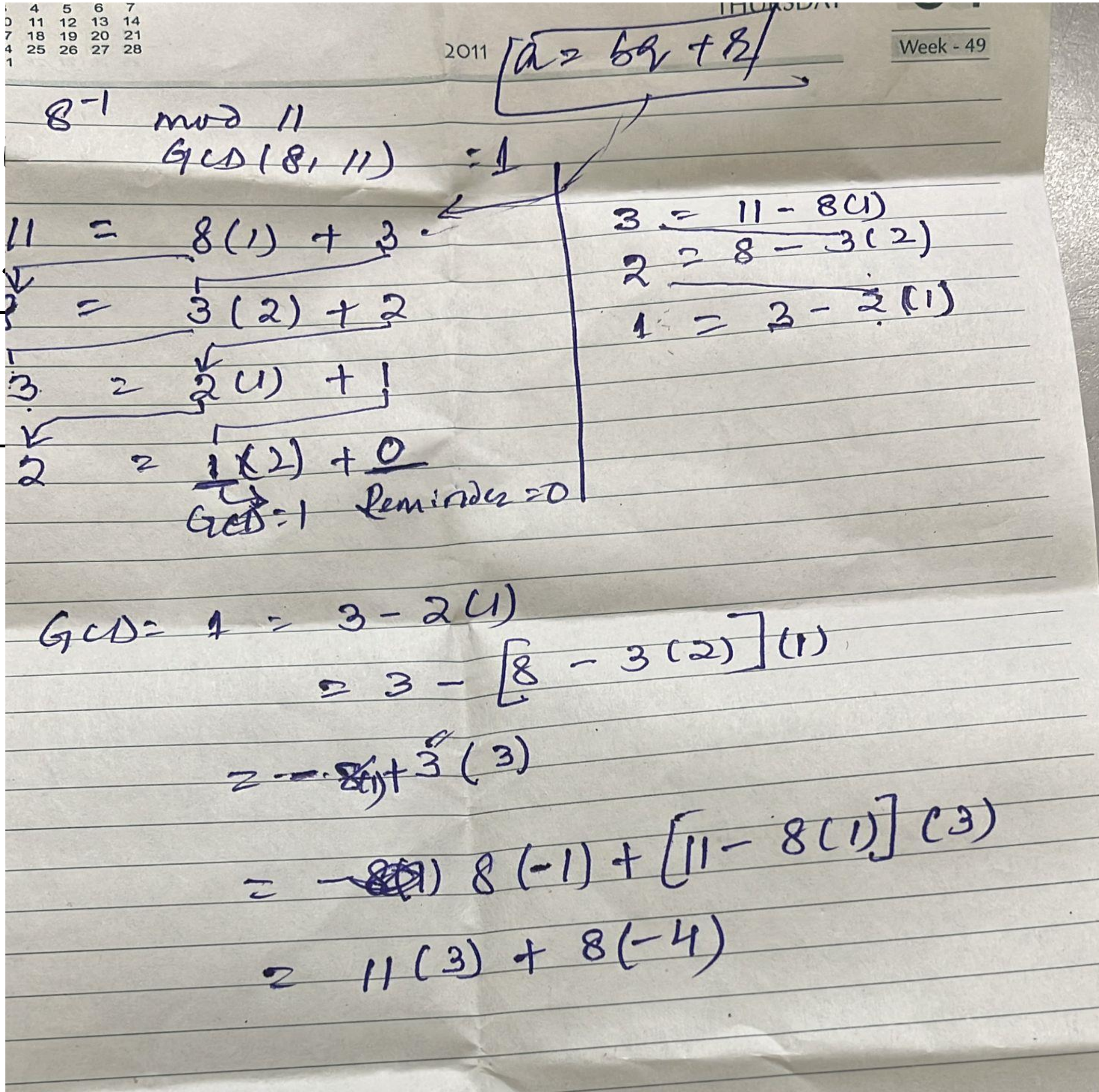
Elementary Number Theory-V

S. Tripathy
IIT Patna

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

Previous Class

- Fi
- E
  - n that r.a + s.b
  -



2011 Week - 49

$8^{-1} \bmod 11$

$GCD(8, 11) = 1$

$\boxed{a = bq + r}$

$11 = 8(1) + 3$

$8 = 3(2) + 2$

$3 = 2(1) + 1$

$2 = 1(2) + 0$

GCD = 1 Reminder = 0

$3 = 11 - 8(1)$

$2 = 8 - 3(2)$

$1 = 3 - 2(1)$

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

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

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

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

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

Fast Exponential: Square and multiply

Compute 30^{37} (mod 77)

Find x^c mod n
C as bit string: $b_{k-1} \ldots b_0$
z = 1
For i = k-1 downto 0 do
    $z = z^2 \bmod n$
    if bi= 1 then
    z = z * x mod n
Endfor

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

Chinese Remainder Theorem

- used to speed up modulo computations
- working modulo a product of numbers
  - eg. mod $M = m_1m_2..m_k$
- Chinese Remainder theorem lets us work in each moduli m_i separately
- since computational cost is proportional to size, this is faster than working in the full modulus M

- can implement CRT in several ways
- to compute (A mod M) can firstly compute all (a_i mod m_i) separately and then combine results to get answer using:

Chinese Remainder Theorem (Contd.)

- Given $x \equiv b_i \bmod m_i$ to solve for mod N, $N = \prod m_i$
- Algo:
  - 1. Solve for each $(N/m_i).\ y_i \equiv 1 \bmod m_{i\ i.e}$
    $y = (N/m_i)$ inverse modulo m_i
  - 2. $A \equiv \Sigma_i N/m_i\ \ b_i \, .\, y_i \bmod N$
- Example: Given $x \equiv 1 \bmod 5$ and $x \equiv 10 \bmod 11$
  - Compute $x \equiv ?$ Mod 55

Chinese Remainder Theorem (Contd.)

- Given $x \equiv b_i \bmod m_i$ to solve for mod N, $N = \Pi\, m_i$
- Algo:
  - 1. Solve for each $(N/m_i).\ y_i \equiv 1 \bmod m_{i\ i.e}$
    $y = (N/m_i)$ inverse modulo m_i
  - 2. $A \equiv \Sigma_i N/m_i\ \ b_i \cdot y_i \bmod N$
- Example: Given $x \equiv 1 \bmod 5$ and $x \equiv 10 \bmod 11$
  - Compute $x \equiv ?$ Mod 55
  - Ans: 21 mod 55

- Find $x \equiv (2,3,2) \pmod{(3,5,7)}$ respectively.
- Sol:

Example

i	m_i	b_i	M_i	$y_i = M_i^{-1} \pmod{m_i}$	$b_i M_i y_i$
1	3	2	m/3=35	$35\, y_1 \equiv 1 \pmod 3$ $\Rightarrow$ -1	2 x 35 x -1
2	5	3	m/5=21	$21\, y_2 \equiv 1 \pmod 5$ $\Rightarrow$ 1	3 x 21 x 1
3	7	2	m/7=15	$15\, y_3 \equiv 1 \pmod 7$ $\Rightarrow$ 1	2 x 15 x 1
	M = 105				x = -70 + 63 + 30 = 23.

Modular e'th roots

We know how to solve modular **linear** equations:

$$a \cdot x + b = 0 \quad \text{in } Z_N$$

Solution: $x = -b \cdot a^{-1}$ in Z_N

What about higher degree polynomials?

Example: Let p be a prime and $c \in Z_p$.

Can we solve:

$$x^2 - c = 0 \quad , \quad y^3 - c = 0 \quad , \quad z^{37} - c = 0 \quad \text{in } Z_p$$

Modular e'th roots

Let p be a prime and $c \in Z_p$.

__Def__: $x \in Z_p$ s.t. $x^e = c$ in Z_p is called an __e'th root__ of c .

Examples:

$7^{1/3} = 6$ in $\mathbb{Z}_{11}$ **$6^3 = 216 = 7$ in Z_{11}**

$3^{1/2} = 5$ in $\mathbb{Z}_{11}$

$1^{1/3} = 1$ in $\mathbb{Z}_{11}$

$2^{1/2}$ does not exist in $\mathbb{Z}_{11}$

How to Compute e^{th} root?

When does $c^{1/e}$ **in** Z_p exist?

If $\gcd(e, p-1) = 1$, then

$c^{1/e}$ exists in Z_p for all c in $(Z_p)^*$.

Proof: let $d = e^{-1}$ **in** Z_{p-1}. i.e, $d \cdot e = 1$ in Z_{p-1} $\Rightarrow$

$c^d = c^{1/e}$ **in** Z_p

The case e=2: square roots

If p is an odd prime then $\gcd(2, p-1) \neq 1$

x −x

Fact: in $\mathbb{Z}_p^*$, $x \longrightarrow x^2$ is a 2-to-1 function

x^2

Example: in $\mathbb{Z}_{11}^*$:

1	10	2	9	3	8	4	7	5	6
1		4		9		5		3	

Def: x in $\mathbb{Z}_p$ is a **quadratic residue** (Q.R.) if it has a square root in $\mathbb{Z}_p$

p odd prime $\Rightarrow$ the # of Q.R. in $\mathbb{Z}_p$ is (p-1)/2 + 1

Euler's theorem

Thm: x in $(Z_p)^*$ is a Q.R. $\iff$ $x^{(p-1)/2} = 1$ in Z_p (p odd prime)

Example:

in $\mathbb{Z}_{11}$	:	1^5,	2^5,	3^5,	4^5,	5^5,	6^5,	7^5,	8^5,	9^5,	10^5
=		1	-1	1	1	1,	-1,	-1,	-1,	1,	-1

Note: $x \neq 0 \Rightarrow x^{(p-1)/2} = (x^{p-1})^{1/2} = 1^{1/2} \in \{ 1, -1 \}$ in Z_p

Def: $x^{(p-1)/2}$ is called the **Legendre Symbol** of x over p

Computing square roots mod p

Suppose $p = 3 \pmod 4)$

Lemma: if $c \in (Z_p)^*$ is Q.R. then $\sqrt{c} = c^{(p+1)/4}$ in Z_p

Proof: $\left[c^{\frac{p+1}{4}}\right]^2 = c^{\frac{p+1}{2}} = \underbrace{c^{\frac{p-1}{2}}}_{=1} \cdot c = c$ in $\mathbb{Z}_p$

When $p = 1 \pmod 4$, can also be a bit harder nad may be solved using randomized algorithm.

Thanks