# Homework Assignment 03

Machiry Aravind Kumar

UCSB

## 1 Problem 1

Consider the exponent d = 49 = (110001). Show the steps and all intermediate powers in the computation of $m^d$ for the algorithms

### 1.1 the left-to-right binary method

### 1.2 the right-to-left binary method

### 1.3 the square-and-multiply-always algorithm

$R_0 = 1, R_1 = 1$

| i | $d_i$ | b | $R_0$ | $R_b$ |
|---|---|---|---|---|
| 5 | 1 | 0 | $R_0 = 1^2 (modN)$ | $R_0 = 1.m(modN)$ |
| 4 | 1 | 0 | $R_0 = m^2 (modN)$ | $R_0 = m^2.m(modN)$ |
| 3 | 0 | 1 | $R_0 = (m^3)^2 (modN)$ | $R_1 = 1.m(modN)$ |
| 2 | 0 | 1 | $R_0 = (m^6)^2 (modN)$ | $R_1 = m.m(modN)$ |
| 1 | 0 | 1 | $R_0 = (m^{12})^2 (modN)$ | $R_1 = m^2.m(modN)$ |
| 0 | 1 | 0 | $R_0 = (m^{24})^2 (modN)$ | $R_0 = m^{48}.m(modN)$ |

$R_0 = m^{49} modN$

### 1.4 the Montgomery powering ladder

$R_0 = 1, R_1 = m$

| i | $d_i$ | b | $R_b$ | $R_{d_i}$ |
|---|---|---|---|---|
| 5 | 1 | 0 | $R_0 = 1.m(modN)$ | $R_1 = m^2 (modN)$ |
| 4 | 1 | 0 | $R_0 = m.m^2 (modN)$ | $R_1 = (m^2)^2 (modN)$ |
| 3 | 0 | 1 | $R_1 = m^3.m^4 (modN)$ | $R_0 = (m^3)^2 (modN)$ |
| 2 | 0 | 1 | $R_1 = m^6.m^7 (modN)$ | $R_0 = (m^6)^2 (modN)$ |
| 1 | 0 | 1 | $R_1 = m^{12}.m^{13} (modN)$ | $R_0 = (m^{12})^2 (modN)$ |
| 0 | 1 | 0 | $R_0 = m^{24}.m^{25} (modN)$ | $R_1 = (m^{25})^2 (modN)$ |

$R_0 = m^{49} modN$

## 1.5 the Atomic square-and-multiply algorithm

## 1.6 the Atomic right-to-left algorithm

## 1.7 Binary method

| i | $e_i$ | Step 2a | Step 2b |
|---|---|---|---|
| 6 | 0 | $(\mathrm{M})^2 = M^2$ | $\mathrm{M}^2$ |
| 5 | 0 | $(\mathrm{M}^2)^2 = M^4$ | $\mathrm{M}^4$ |
| 4 | 0 | $(\mathrm{M}^4)^2 = M^8$ | $\mathrm{M}^8$ |
| 3 | 1 | $(\mathrm{M}^8)^2 = M^{16}$ | $\mathrm{M}^{16}.M = M^{17}$ |
| 2 | 1 | $(\mathrm{M}^{17})^2 = M^{34}$ | $\mathrm{M}^{34}.M = M^{35}$ |
| 1 | 1 | $(\mathrm{M}^{35})^2 = M^{70}$ | $\mathrm{M}^{70}.M = M^{71}$ |
| 0 | 1 | $(\mathrm{M}^{71})^2 = M^{142}$ | $\mathrm{M}^{142}.M = M^{143}$ |

Addition chain = 1 2 4 8 16 17 34 35 70 71 142 143, Length = 12.

## 1.8 m-ary method

### 1.8.1 For d=2

| bits | w | $\mathrm{M}^w$ |
|---|---|---|
| 00 | 0 | 1 |
| 01 | 1 | M |
| 10 | 2 | $\mathrm{M.M} = \mathrm{M}^2$ |
| 11 | 3 | $\mathrm{M}^2.M = M^3$ |

| i | $F_i$ | Step 4a | Step 4b |
|---|---|---|---|
| 2 | 00 | $(\mathrm{M}^2)^4 = M^8$ | $\mathrm{M}^8$ |
| 1 | 11 | $(\mathrm{M}^8)^4 = M^{32}$ | $\mathrm{M}^{32}.M^3 = M^{35}$ |
| 0 | 11 | $(\mathrm{M}^{35})^4 = M^{140}$ | $\mathrm{M}^{140}.M^3 = M^{143}$ |

Addition chain = 1 2 3 4 8 16 32 35 70 140 143, Length = 11.

### 1.8.2 For d=4

| bits | w | $M^w$ |
|---|---|---|
| 0000 | 0 | 1 |
| 0001 | 1 | M |
| 0010 | 2 | $M.M = M^2$ |
| 0011 | 3 | $M^2.M = M^3$ |
| 0100 | 4 | $M^3.M = M^4$ |
| 0101 | 5 | $M^4.M = M^5$ |
| 0110 | 6 | $M^5.M = M^6$ |
| 0111 | 7 | $M^6.M = M^7$ |
| 1000 | 8 | $M^7.M = M^8$ |
| 1001 | 9 | $M^8.M = M^9$ |
| 1010 | 10 | $M^9.M = M^{10}$ |
| 1011 | 11 | $M^{10}.M = M^{11}$ |
| 1100 | 12 | $M^{11}.M = M^{12}$ |
| 1101 | 13 | $M^{12}.M = M^{13}$ |
| 1110 | 14 | $M^{13}.M = M^{14}$ |
| 1111 | 15 | $M^{14}.M = M^{15}$ |

| i | $F_i$ | Step 4a | Step 4b |
|---|---|---|---|
| 0 | 1111 | $(M^8)^{16} = M^{128}$ | $M^{128}.M^{15} = M^{143}$ |

Addition chain = 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 32 64 128 143, Length = 20.

## 1.9 Factor Method

Compute: $M \rightarrow M^2$
$Assign : a = M^2$
$Compute : a \rightarrow a^2 \rightarrow a^4 \rightarrow a^5$
$Assign : b = a^5 = M^{10}$
$Compute : b.M \rightarrow M^{11}$
$Assign : c = M^{11}$
$Compute : c \rightarrow c^2 \rightarrow c^3$
$Assign : d = c^3 = (M^{11})^3$
$Compute : d \rightarrow d^2 \rightarrow d^4$
$Assign : e = d^4 = (M^{11})^{12}$
$Compute : e.c \rightarrow (M^{11})^{13} = M^{143}$
Addition chain = 1 2 4 8 10 11 22 33 66 132 143, Length = 11.

## 1.10 Power Tree Method

A tree of height 11 leads to 143 as its leaf node. Refer code `mk_tree.py` for the details. The path from the root is: 1 2 3 5 7 14 21 35 70 140 143. Addition chain is same as this path.
Addition chain = 1 2 3 5 7 14 21 35 70 140 143, Length = 11.

## 1.11 Canonical Recording for d=1

Truth table for canonical recording is as shown below:

| $c_i$ | $e_{i+1}$ | $e_i$ | $c_{i+1}$ | $f_i$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 1 |
| 0 | 1 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 | $\bar{1}$ |
| 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 1 | 1 | 0 |
| 1 | 1 | 0 | 1 | $\bar{1}$ |
| 1 | 1 | 1 | 1 | 0 |

Using truth table, recording for given number is:

| $c_i$ | $e_{i+1}$ | $e_i$ | $c_{i+1}$ | $f_i$ |
|---|---|---|---|---|
| 0 | 1 | 1 | 1 | $\bar{1}$ |
| 1 | 1 | 1 | 1 | 0 |
| 1 | 1 | 1 | 1 | 0 |
| 1 | 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 0 | 1 |
| 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 1 |

$1001000\bar{1} = 2^7 + 2^4 - 2^0 = 143$

Computing the exponent:

| i | $f_i$ | Step 2a | Step 2b |
|---|---|---|---|
| 7 | 1 | M | M |
| 6 | 0 | $(\mathrm{M})^2 = M^2$ | $\mathrm{M}^2$ |
| 5 | 0 | $(\mathrm{M}^2)^2 = M^4$ | $\mathrm{M}^4$ |
| 4 | 1 | $(\mathrm{M}^4)^2 = M^8$ | $\mathrm{M}^8.M = M^9$ |
| 3 | 0 | $(\mathrm{M}^9)^2 = M^{18}$ | $\mathrm{M}^{18}$ |
| 2 | 0 | $(\mathrm{M}^{18})^2 = M^{36}$ | $\mathrm{M}^{36}$ |
| 1 | 0 | $(\mathrm{M}^{36})^2 = M^{72}$ | $\mathrm{M}^{72}$ |
| 0 | $\bar{1}$ | $(\mathrm{M}^{72})^2 = M^{144}$ | $\mathrm{M}^{144}.\mathrm{M}^{-1} = \mathrm{M}^{143}$ |

Addition chain: 1 2 4 8 9 18 36 72 144 143, Length = 10.

## 2 Illustrate the steps of the standard multiplication algorithm for computing c =a * b = 456 * 555

| i | j | Step | (C,S) | Partial t |
|---|---|---|---|---|
| 0 | 0 | $t_0 + a_0b_0 + C$ | (0,*) | 000000 |
| | | 0 + 6*5 + 0 | (3,0) | 00000**0** |
| | 1 | $t_1 + a_1b_0 + C$ | | |
| | | 0 + 5*5 + 3 | (2,8) | 0000**8**0 |
| | 2 | $t_2 + a_2b_0 + C$ | | |
| | | 0 + 4*5 + 2 | (2,2) | 000**2**80 |
| | | | | 00**2**280 |
| 1 | 0 | $t_1 + a_0b_1 + C$ | (0,*) | |
| | | 8 + 6*5 + 0 | (3,8) | 0022**8**0 |
| | 1 | $t_2 + a_1b_1 + C$ | | |
| | | 2 + 5*5 + 3 | (3,0) | 002**0**80 |
| | 2 | $t_3 + a_2b_1 + C$ | | |
| | | 2 + 4*5 + 3 | (2,5) | 00**5**080 |
| | | | | 0**2**5080 |
| 2 | 0 | $t_2 + a_0b_2 + C$ | (0,*) | |
| | | 0 + 6*5 + 0 | (3,0) | 025**0**80 |
| | 1 | $t_3 + a_1b_2 + C$ | | |
| | | 5 + 5*5 + 3 | (3,3) | 02**3**080 |
| | 2 | $t_4 + a_2b_2 + C$ | | |
| | | 2 + 4*5 + 3 | (2,5) | 0**5**3080 |
| | | | | **2**53080 |

## 3 Illustrate the steps of the standard squaring algorithm for computing c =a * a = 456 * 456

| i | j | Step | (C,S) | Partial t |
|---|---|---|---|---|
| 0 | 1 | $t_0 + a_0a_0$ | | 000000 |
| | | 0 + 6*6 | (3,6) | 00000**6** |
| | | $t_1 + 2a_1a_0 + C$ | (3,*) | 000006 |
| | | 0 + 2*5*6 + 3 | (6,3) | 0000**3**6 |
| 0 | 2 | $t_2 + 2a_2a_0 + C$ | (6,*) | 000036 |
| | | 0 + 2*4*6 + 6 | (5,4) | 000**4**36 |
| | | | | 00**5**436 |
| 1 | 2 | $t_2 + a_1a_1$ | | 005436 |
| | | 4 + 5*5 | (2,9) | 005**9**36 |
| | | $t_3 + 2a_2a_1 + C$ | (2,*) | 005936 |
| | | 5 + 2*4*5 + 2 | (4,7) | 00**7**936 |
| | | | | 0**4**7936 |
| 2 | 2 | $t_4 + a_2a_2$ | | 047936 |
| | | 4 + 4*4 | (2,0) | 0**0**7936 |
| | | | | **2**07936 |

## 4 Let r = 32, n = 21, a = 13, and b = 15. Compute $c = a * b * r^{-1}$ mod n using the standard Montgomery multiplication algorithm. Illustrate the steps and give all temporary results

| iteration | q | $g_0$ | $g_1$ | $u_0$ | $u_1$ | $v_0$ | $v_1$ |
|---|---|---|---|---|---|---|---|
| 0 | - | 32 | 21 | 1 | 0 | 0 | 1 |
| 1 | 1 | 21 | 11 | 0 | 1 | 1 | -1 |
| 2 | 1 | 11 | 10 | 1 | -1 | -1 | 2 |
| 3 | 1 | 10 | 1 | -1 | 2 | 2 | -3 |
| 4 | 10 | 1 | 0 | 2 | -21 | -3 | 32 |
| | | • | | • | | • | |

From Table 4, GCD = 1, $r^{-1}$ = 2, $n'$ = 3.
Consider $\overline{x}$ = a = 13, such that x = $\overline{x} * r^{-1}$ mod n = 5. $\overline{y}$ = b = 15, such that y = $\overline{y} * r^{-1}$ mod n = 9.
Now, $a * b * r^{-1}$ mod n is same as $\overline{x} * \overline{y} * r^{-1}$ mod n.
So, $a * b * r^{-1}$ mod n = $\overline{x} * \overline{y} * r^{-1}$ mod n = MonPro($\overline{x}$ = 13,$\overline{y}$ = 15).

### 4.1 function MonPro($\overline{a}$ = 13 , $\overline{b}$ = 15)

1. t = 13*15 = 195
2. m = (195*3) mod 32 = 9
3. u = (195 + 9 * 21) / 32 = 384/32 = 12
4. 12 < 21 **return** 12

Final result is : 12.

## 5 Let p = 29, a = 23, and g = 10. Compute $g^a$ (mod p) using the binary method of exponentiation and the Montgomery multiplication where r = 32. Show the steps and temporary values.

Consider n=p=29, M=g=10, e=a=23.

| iteration | q | $g_0$ | $g_1$ | $u_0$ | $u_1$ | $v_0$ | $v_1$ |
|---|---|---|---|---|---|---|---|
| 0 | - | 32 | 29 | 1 | 0 | 0 | 1 |
| 1 | 1 | 29 | 3 | 0 | 1 | 1 | -1 |
| 2 | 9 | 3 | 2 | 1 | -9 | -1 | 10 |
| 3 | 1 | 2 | 1 | -9 | 10 | 10 | -11 |
| 4 | 2 | 1 | 0 | 10 | -29 | -11 | 32 |
| | | • | | • | | • | |

From Table 5, GCD = 1, $r^{-1}$ = 10, $n'$ = 11.

- Step 2

  $\overline{M}$ = M * r mod n = 10 * 32 mod 29 = 1

- Step 3

  $\overline{C}$ = 1 * r mod n = 1 * 32 mod 29 = 3

- Step 4

| $e_i$ | Step 5 | Step 6 |
|---|---|---|
| 1 | MonPro(3,3) = 3 | MonPro(1,3) = 1 |
| 0 | MonPro(1,1) = 10 | |
| 1 | MonPro(10,10) = 14 | MonPro(1,14) = 24 |
| 1 | MonPro(24,24) = 18 | MonPro(1,18) = 6 |
| 1 | MonPro(6,6) = 12 | MonPro(1,12) = 4 |

$MonPro(3,3)$
t = 3 * 3 = 9
m = 9 * 11 mod 32 = 3
u = (9 + 3 * 29) / 32 = 3

$MonPro(1,3)$
t = 1 * 3 = 3
m = 3 * 11 mod 32 = 1
u = (3 + 1 * 29) / 32 = 1

$MonPro(1,1)$
t = 1 * 1 = 1
m = 1 * 11 mod 32 = 11
u = (1 + 11 * 29) / 32 = 10

$MonPro(10,10)$
t = 10 * 10 = 100
m = 100 * 11 mod 32 = 12
u = (100 + 12 * 29) / 32 = 14

$MonPro(1,14)$
t = 1 * 14 = 14
m = 14 * 11 mod 32 = 26
u = (14 + 26 * 29) / 32 = 24

$MonPro(24,24)$
t = 24 * 24 = 576
m = 576 * 11 mod 32 = 0
u = (576 + 0 * 29) / 32 = 18

$MonPro(1,18)$
t = 1 * 18 = 18
m = 18 * 11 mod 32 = 6
u = (18 + 6 * 29) / 32 = 6

$MonPro(6, 6)$
t = 6 * 6 = 36
m = 36 * 11 mod 32 = 12
u = (36 + 12 * 29) / 32 = 12

$MonPro(1, 12)$
t = 1 * 12 = 12
m = 12 * 11 mod 32 = 4
u = (12 + 4 * 29) / 32 = 4

- Step 7
  C = MonPro(4,1) = 11

Result of $10^{23}$ (mod 29) = **11**

# 6 Let an RSA key be determined by the parameters {p,q,n,e,d} = {17,23,391,29,85}. Compute S = $M^d$ (mod n) for M = 175 with and without the Chinese remainder theorem and the binary exponentiation.

## 6.1 Chinese remainder theorem

$d_1$ = 85 mod (16) = 5
$d_2$ = 85 mod (22) = 19

| iteration | quotient | $g_0$ | $g_1$ | $u_0$ | $u_1$ | $v_0$ | $v_1$ |
|---|---|---|---|---|---|---|---|
| 0 | - | 23 | 17 | 1 | 0 | 0 | 1 |
| 1 | 1 | 17 | 6 | 0 | 1 | 1 | -1 |
| 2 | 2 | 6 | 5 | 1 | -2 | -1 | 3 |
| 3 | 1 | 5 | 1 | -2 | 3 | 3 | -4 |
| 4 | 5 | 1 | 0 | 3 | -17 | -4 | 23 |
| | | • | | • | | • | |

In Table 6.1, Initial values of $g_0$ = q = 23 and $g_1$ = p = 17. This $p^{-1}$ = -4 and $q^{-1}$ = 3.
$M_1 = M^{d_1}$ mod p = $175^5$ mod 17 = 14.
$M_2 = M^{d_2}$ mod q = $175^{19}$ mod 23 = 10.
S = $M_1$ + p *(($M_2$ - $M_1$) * $p^{-1}$ mod q) = 14 + 17*((10-14)*-4 mod 23) = 14 + 272 = **286**.

## 6.2 Binary Exponentiation.

Representing 85 in binary results in: 1 0 1 0 1 0 1
Following table shows computation of RSA decryption using binary exponentiation.

| i | $e_i$ | Step 2a | Step 2b |
|---|---|---|---|
| 6 | 0 | $((175)^2)$ mod 391 = 127 | 127 |
| 5 | 1 | $((127)^2)$ mod 391 = 98 | 98*175 mod 391 = 337 |
| 4 | 0 | $((337)^2)$ mod 391 = 179 | 179 |
| 3 | 1 | $((179)^2)$ mod 391 = 370 | 370*175 mod 391 = 235 |
| 1 | 0 | $((235)^2)$ mod 391 = 94 | 94 |
| 0 | 1 | $((94)^2)$ mod 391 = 234 | 234*175 mod 391 = **286** |