

ECE 679
HomeWork #1 Due: 4/28/03

Peroly Natesan
930-30-6518

1) Let $e=(1001\ 1111\ 1010\ 1000\ 1100\ 0100\ 0110\ 0011)$ the exponent. Illustrate the addition chains produced by each one of the following algorithms. Write down the length of each addition chain.

A. m-ary method for $d=1,2,3,4$

CASE: $d = 1$:

calculate $M \cdot M = M^2$

e_i		
1	M	
0	$(M)2 = M2$	
0	$(M2)2 = M4$	
1	$(M4)2 = M8$	$M8 \cdot M = M9$
1	$(M9)2 = M18$	$M18 \cdot M = M19$
1	$(M19)2 = M38$	$M38 \cdot M = M39$
1	$(M39)2 = M78$	$M78 \cdot M = M79$
1	$(M79)2 = M158$	$M158 \cdot M = M159$
1	$(M159)2 = M318$	$M318 \cdot M = M319$
0	$(M319)2 = M638$	
1	$(M638)2 = M1276$	$M1276 \cdot M = M1277$
0	$(M1277)2 = M2554$	
1	$(M2554)2 = M5108$	$M5108 \cdot M = M5109$
0	$(M5109)2 = M10218$	
0	$(M10218)2 = M20436$	
0	$(M20436)2 = M40872$	
1	$(M40872)2 = M81744$	$M81744 \cdot M = M81745$
1	$(M81745)2 = M163490$	$M163490 \cdot M =$ $M163491$
0	$(M163491)2 = M326892$	
0	$(M326892)2 = M653964$	
0	$(M653964)2 =$ $M1307928$	
1	$(M1307928)2 =$ $M2615856$	$M2615856 \cdot M =$ $M2615857$
0	$(M2615857)2 =$ $M5231714$	
0	$(M5231714)2 =$	

	M10463428	
0	(M10463428) ² = M20926856	
1	(M20926856) ² = M41853712	M41853712 · M = M41853713
1	(M41853713) ² = M83707426	M83707426 · M = M83707427
0	(M83707427) ² = M167414854	
0	(M167414854) ² = M334829708	
0	(M334829708) ² = M669659416	
1	(M669659416) ² = M1339318832	M1339318832 · M = M1339318833
1	(M1339318833) ² = M2678637666	M2678637666 · M = M_2678637667

total multiplications = 0+32+15 = **47**

- 1 Preprocessing multiplications = $2^d - 1 = 2 - 2 = 0$
- 2 Squarings = $((k/d) - 1) \cdot d = k - d = 32 - 1 = 31$
- 3 Multiplications = $(m - 1/m) \cdot (k/d - 1) = 31/2 = 16$
- 4 Total Multiplications = $0 + 31 + 16 = 47$

CASE: d = 2.

Pre-processing:

00 M0 = 1

01 M1 = M

10 M · M = M2

11 M2 · M = M3

e _i		
10	M2	
01	(M2) ⁴ = M8	M8 · M1 = M9
11	(M9) ⁴ = M36	M36 · M3 = M39
11	(M39) ⁴ = M156	M156 · M3 = M159
10	(M159) ⁴ = M636	M636 · M2 = M638
10	(M638) ⁴ = M2552	M2552 · M2 = M2554
10	(M2554) ⁴ = M10216	M10208 · M2 = M10218
00	(M10218) ⁴ = M40872	M40872 · M0 = M40872
11	(M40872) ⁴ = M163488	M163488 · M3 = M163491

00	$(M163491)^4 = M653964$	$M653964 \cdot M0 = M653964$
01	$(M653964)^4 = M2615856$	$M2615856 \cdot M1 = M2615857$
00	$(M2615857)^4 = M10463428$	$M10463428 \cdot M0 = M10463428$
01	$(M10463428)^4 = M41852712$	$M41853712 \cdot M1 = M41853713$
10	$(M41853713)^4 = M167414852$	$M167414852 \cdot M2 = M167414854$
00	$(M167414854)^4 = M669659416$	$M669659416 \cdot M0 = M669659416$
11	$(M669659416)^4 = M2678637664$	$M2678637664 \cdot M3 = M_{2678637667}$

total multiplications = $2+30+11 = 43$

- 1 Preprocessing multiplications = $2^d - 2 = 4 - 2 = 2$
- 2 Squarings = $((k/d) - 1) \cdot d = k - d = 32 - 2 = 30$
- 3 Multiplications = $(m - 1/m) \cdot (k/d - 1) = 45/4 = 11$
- 4 Total Multiplications = $2 + 30 + 11 = 43$

CASE: d=3

Pre-processing:

000 $M0 = 1$

001 $M1 = M$

010 $M \cdot M = M2$

.

.

110 $M3 \cdot M3 = M6$

111 $M4 \cdot M3 = M7$

e_i		
010	$M2$	
011	$(M2)^8 = M16$	$M16 \cdot M3 = M19$
111	$(M19)^8 = M152$	$M152 \cdot M7 = M159$
101	$(M159)^8 = M1272$	$M1272 \cdot M5 = M1277$
010	$(M1277)^8 = M10216$	$M10216 \cdot M2 = M110218$
001	$(M10218)^8 = M81744$	$M81744 \cdot M1 = M81745$
100	$(M81745)^8 = M653960$	$M653960 \cdot M4 = M653964$
010	$(M653964)^8 = M5231712$	$M5231712 \cdot M2 = M5231714$

001	$(M5231714)_8 = M41852712$	$M41853712 \cdot M1 = M41853713$
100	$(M41853713)_8 = M334829704$	$M334829704 \cdot M4 = M334829708$
011	$(M334829708)_8 = M2678637664$	$M2678637664 \cdot M3 = M_{2678637667}$

total multiplications = $6+30+10 = 46$

- 1 Preprocessing multiplications = $2^d - 2 = 8 - 2 = 6$
- 2 Squarings = $((k/d) - 1) \cdot d = k - d = 32 - 3 = 29$
- 3 Multiplications = $(m - 1/m) \cdot (k/d - 1) = 203/24 = 9$
- 4 Total Multiplications = $6 + 29 + 9 = 44$

CASE: $d = 4$.

Pre-processing:

0000 $M0 = 1$

0001 $M1 = M$

0010 $M \cdot M = M2$

.

.

1110 $M6 \cdot M8 = M14$

1111 $M8 \cdot M7 = M15$

e_i		
1001	M9	
1111	$(M9)_{16} = M144$	$M144 \cdot M15 = M159$
1010	$(M159)_{16} = M2544$	$M2544 \cdot M10 = M2554$
1000	$(M2554)_{16} = M40864$	$M40864 \cdot M8 = M40872$
1100	$(M40872)_{16} = M653952$	$M653952 \cdot M12 = M653964$
0100	$(M653694)_{16} = M10463424$	$M10463424 \cdot M4 = M10463428$
0110	$(M10463428)_{16} = M167414848$	$M167414848 \cdot M6 = M167414854$
0011	$(M167414854)_{16} = M2678637664$	$M2678637664 \cdot M3 = M_{2678637667}$

Total multiplications = $14+28+7 = 49$

- 1 Preprocessing multiplications = $2^d - 2 = 16 - 2 = 14$
- 2 Squarings = $((k/d) - 1) \cdot d = k - d = 32 - 4 = 28$
- 3 Multiplications = $(m - 1/m) \cdot (k/d - 1) = 7$
- 4 Total Multiplications = $14 + 28 + 7 = 49$

B. m-ary method for d=2,3,4 and with reduced preprocessing:

CASE d=2:

Preprocessing steps = 2.

00 $M_0 = 1$

01 $M_1 = M$

10 $M \cdot M = M_2$

11 $M_2 \cdot M = M_3$

number of multiplications = **44** .

i	ei	Step4a	Step4b
14	01	$(M^2)^4 = M^8$	$M^8 \cdot M = M^9$
13	11	M^{36}	M^{39}
12	11	M^{156}	M^{159}
11	10	M^{636}	M^{638}
10	10	M^{2552}	M^{2554}
9	10	M^{10216}	M^{10218}
8	00	M^{40872}	
7	11	M^{163488}	M^{163491}
6	00	M^{653964}	
5	01	$M^{2615856}$	$M^{2615857}$
4	00	$M^{10463428}$	
3	01	$M^{41853712}$	$M^{41853713}$
2	10	$M^{167414852}$	$M^{167414854}$
1	00	$M^{669659416}$	
0	11	$M^{2678637664}$	$M^{2678637667}$

CASE d=3:

Pre-processing:

000 $M_0 = 1$

001 $M_1 = M$

010 $M \cdot M = M_2$

....

111 $M_4 \cdot M_3 = M_7$

preprocessing steps = 5. number of multiplications = **43**.

$M^{FS-1} = M^2$

i	ei	Step4a	Step4b
9	011	$(M^2)^8 = M^{16}$	$M^{16} \cdot M^3 = M^{19}$
8	111	$(M^{19})^8 = M^{152}$	$M^{152} \cdot M^7 = M^{159}$
7	101	M^{1272}	M^{1277}
6	010	M^{10216}	M^{10218}
5	001	M^{81744}	M^{81745}
4	100	M^{653960}	M^{653964}

3	010	$M^{5231712}$	$M^{5231714}$
2	001	$M^{41853712}$	$M^{41853713}$
1	100	$M^{334829704}$	$M^{33482908}$
0	011	$M^{2678637664}$	$M^{2678637667}$

CASE d=4:

Pre-processing:

0000 $M_0 = 1$

0001 $M_1 = M$

0010 $M \cdot M = M_2$

.....

1111 $M_8 \cdot M_7 = M_{15}$

$M_{FS-1} = M_9$

i	e_i	Step4a	Step4b
6	1111	$(M_9)^{16} = M^{144}$	$M^{144} \cdot M^{15} = M^{159}$
5	1010	M^{2544}	M^{2554}
4	1000	M^{40864}	M^{40872}
3	1100	M^{653952}	M^{653964}
2	0100	$M^{10463424}$	$M^{10463428}$
1	0110	$M^{167414848}$	$M^{167414851}$
0	0011	$M^{2678637664}$	$M^{2678637667}$

preprocessing steps = 9. number of multiplications = **45**.

C.CLNW with d=2,3,4:

CASE d = 2:

$e = \underline{10} \underline{01} \underline{11} \underline{11} \underline{10} \underline{10} \underline{10} \underline{00} \underline{11} \underline{00} \underline{01} \underline{00} \underline{01} \underline{10} \underline{00} \underline{11}$

e_i		
10	M_2	
01	$(M_2)_4 = M_8$	$M_8 \cdot M_1 = M_9$
11	$(M_9)_4 = M_{36}$	$M_{36} \cdot M_3 = M_{39}$
11	$(M_{39})_4 = M_{156}$	$M_{156} \cdot M_3 = M_{159}$
10	$(M_{159})_4 = M_{636}$	$M_{636} \cdot M_2 = M_{638}$
10	$(M_{638})_4 = M_{2552}$	$M_{2552} \cdot M_2 = M_{2554}$
10	$(M_{2554})_4 = M_{10216}$	$M_{10208} \cdot M_2 =$ M_{10218}
00	$(M_{10218})_4 = M_{40872}$	$M_{40872} \cdot M_0 =$ M_{40872}
11	$(M_{40872})_4 = M_{163488}$	$M_{163488} \cdot M_3 =$ M_{163491}

00	$(M163491)_4 = M653964$	$M653964 \cdot M0 = M653964$
01	$(M653964)_4 = M2615856$	$M2615856 \cdot M1 = M2615857$
00	$(M2615857)_4 = M10463428$	$M10463428 \cdot M0 = M10463428$
01	$(M10463428)_4 = M41852712$	$M41853712 \cdot M1 = M41853713$
10	$(M41853713)_4 = M167414852$	$M167414852 \cdot M2 = M167414854$
00	$(M167414854)_4 = M669659416$	$M669659416 \cdot M0 = M669659416$
11	$(M669659416)_4 = M2678637664$	$M2678637664 \cdot M3 = M_{2678637667}$

multiplications = $30 + 1 + 11 = 42$

CASE d = 3:

e = 010 011 111 101 010 001 100 010 001 100 011

e_i		
100	M4	
111	$(M4)_8$	$M32 \cdot M7$
111	$(M39)_8$	$M312 \cdot M7$
0	$(M319)_8$	M638
101	$(M638)_8$	$M5104 \cdot M5$
000	$(M5109)_8$	M40872
110	$(M40872)_8$	$M326976 \cdot M6$
00	$(M326982)_8$	M1307928
100	$(M1307928)_8$	$M10463424 \cdot M4$
011	$(M10463428)_8$	$M83707424 \cdot M3$
00	$(M83707427)_4$	M334829709
011	$M(334829709)_8$	$M2678637664 \cdot M3 = M_{2678637667}$

total multiplications = **41**

d = 4

e = 1001 1111 1010 1000 1100 0100 0110 0011

e_i		
1001	M9	
1111	$(M9)_{16} = M144$	$M144 \cdot M15 = M159$
1010	$(M159)_{16} = M2544$	$M2544 \cdot M10 = M2554$

1000	(M2554)16 = M40864	M40864 · M8 = M40872
1100	(M40872)16 = M653952	M653952 · M12 = M653964
0100	(M653694)16 = M10463424	M10463424 · M4 = M10463428
0110	(M10463428)16 = M167414848	M167414848 · M6 = M167414854
0011	(M167414854)16 = M2678637664	M2678637664 · M3 = M_2678637667

multiplications = **38**

D. VLNW with d=4 and q=2,3:

CASE d = 4 and q = 2.:

e = 1001 1111 1010 1 000 11 000 1 000 11 000 11

e _i		
1001	M9	
1111	(M9)16	M144 · M15
1010	(M159)16	M2544 · M10
1	(M2554)2	M5108 · M
000	(M5109)8	M40872
11	(M40872)4	M163488 · M3
000	(M163491)8	M1307928
1	(M1307928)2	M2615856 · M
000	(M2615857)8	M20926856
11	(M20926856)4	M83707424.M3
000	(M83707427)8	M669659416
11	(M669659416)4	M2678637664.M3

multiplications = **42**

CASE d = 4 and q = 3:

e = 1001 1111 1010 1 000 11 000 1 000 11 00 011

e _i		
1001	M9	
1111	(M9)16	M144 · M15
1010	(M159)16	M2544 · M10
1	(M2554)2	M5108 · M
000	(M5109)8	M40872
11	(M40872)4	M163488 · M3

000	(M163491)8	M1307928
1	(M1307928)2	M2615856 · M
000	(M2615857)8	M20926856
11	(M20926856)4	M83707424.M3
00	(M83707427)4	M334829708
011	(M334829708)8	M2678637664.M3

Total multiplications = 28 + 7 = 35 + 7(reduced preprocessing) = **42**

E. Factor method:

$e = 2678637667$

Factors of e are 233, 547 and 21017.

I am using,

$e = 233 \cdot 11496299$.

Compute $y \rightarrow y^2 \rightarrow y^4 \rightarrow y^8 \rightarrow y^{16} \rightarrow y^{32} \rightarrow y^{64} \rightarrow y^{128} \rightarrow y^{128} \cdot y^{64} \cdot y^{32} \cdot y^8 \cdot y = y^{233}$

Assign $y := M^{233}$;

Compute $y \rightarrow y^{233}$;

Assign $z := y^{233}$;

Compute $z \rightarrow z^2 \rightarrow z^4 \rightarrow z^8 \rightarrow z^{16} \rightarrow z^{32} \rightarrow z^{64} \rightarrow z^{128} \rightarrow z^{256} \rightarrow z^{512} \rightarrow z^{1024} \rightarrow z^{2048} \rightarrow z^{4096} \rightarrow z^{8192} \rightarrow z^{16384}$

$z^{16384} \cdot z^{8192} \cdot z^{64} \cdot z^{16} \cdot z^8 \cdot z^4 \cdot z^2 = M^{11496299}$

Compute $z^{16384} \rightarrow (z^{16384}y) = M^{2678637667}$

Total = (11 + 1 + 14 + 6) = **32** multiplications.

F. Booth recoding for $d=1,2,3,4$:

$e = 2678637667$

$2^{32} = 4294967296$

$2^{32} - e = 1616329629(\text{bin}) = 001100000010101110011101110011101$

Recoded $e = 1 \underline{0110} \underline{0000} \underline{0101} \underline{0111} \underline{0011} \underline{1011} \underline{1001} \underline{1101}$

Underline in recoded e implies 1 overbar.

CASE $d = 1$:

e_i		
1	M	
0	(M)2	
$\bar{1}$	(M2)2	$M^4 \cdot M^{-1} = M^3$
$\bar{\bar{1}}$	(M3)2	$M^6 \cdot M^{-1}$
0	(M5)2	M10
0	(M10)2	M20
0	(M20)2	M40
0	(M40)2	M80
0	(M80)2	M160
0	(M160)2	M320

$\bar{1}$	(M320)2	M640.M-1
0	(M639)2	M1278
$\bar{1}$	(M1278)2	M2556.M-1
0	(M2555)2	M5110
$\bar{1}$	(M5110)2	M10220.M-1
$\bar{1}$	(M10219)2	M20438.M-1
$\bar{1}$	(M20437)	M40874.M-1
0	(M40873)2	M81746
0	(M81746)2	M163492
$\bar{1}$	(M163492)2	M326984.M-1
$\bar{1}$	(M326983)2	M653966.M-1
$\bar{1}$	(M653965)2	M1307930.M-1
0	(M1307929)2	M2615858
$\bar{1}$	(M2615858)2	M5231716.M-1
$\bar{1}$	(M5231715)2	M10463430.M-1
$\bar{1}$	(M10463429)2	M20926858.M-1
0	(M20926857)2	M41853714
0	(M41853714)2	M83707428
$\bar{1}$	(M83707428)2	M167414856.M-1
$\bar{1}$	(M167414855)2	M334829710.M-1
$\bar{1}$	(M334829709)2	M669659418.M-1
0	(M669659417)2	M1339318834
$\bar{1}$	(M1339318834)2	M2678637668 · M-1 = 2678637667

CASE d = 2:

e_i		
10	M2	M2
$\bar{1}\bar{1}$	(M2)4	M8 · M-3
00000	(M5)32	M160
0 $\bar{1}$	(M160)4	M640.M-1
0 $\bar{1}$	(M639)4	M2556.M-1
0 $\bar{1}$	(M2555)4	M10219
$\bar{1}\bar{1}$	(M10219)4	M40876 · M-3
00	(M40873)4	M163492
$\bar{1}\bar{1}$	(M163492)4	M653968.M-3
$\bar{1}0$	(M653965)4	M2615858 · M-2
$\bar{1}\bar{1}$	(M2615858)4	M10463431 · M-3
$\bar{1}0$	(M10463429)4	M41853716 · M-2
0 $\bar{1}$	(M41853714)4	M167414856 · M-1
$\bar{1}\bar{1}$	(M167414855)4	M669659420 · M-3
0 $\bar{1}$	(M669659417)4	M2678637667 · M-1 = 2678637667

CASE d = 3:

e_i		
1 0 $\bar{1}$	M3	
$\bar{1}$ 0 0	(M3)8	M24 · M-4
0000	(M20)16	M320
$\bar{1}$ 0 $\bar{1}$	(M320)8	M2560 · M-5
0	(M2555)2	M5110
$\bar{1}$ $\bar{1}$ $\bar{1}$	(M5110)8	M40880 · M-7
00	(M40873)4	M163492
$\bar{1}$ $\bar{1}$ $\bar{1}$	(M163492)8	M1307936 · M-1
0	(M1307929)2	M2615858
$\bar{1}$ $\bar{1}$ $\bar{1}$	(M2615858)8	M20926864 · M-7
0	(M20926857)4	M41853714
0 $\bar{1}$ $\bar{1}$	M(41853714)8	M334829712 · M-3
$\bar{1}$ 0 $\bar{1}$	M(334829709)8	M2678637672 · M-5 = M2678637667

CASE d = 4:

e_i		
1 0 $\bar{1}$ $\bar{1}$	M5	
00000	(M5)32	M160
0 $\bar{1}$ 0 $\bar{1}$	(M160)16	M2560 · M-5
0 $\bar{1}$ $\bar{1}$ $\bar{1}$	(M2555)16	M40880 · M-7
0 0 $\bar{1}$ $\bar{1}$	(M40873)16	M653968 · M-3
$\bar{1}$ 0 $\bar{1}$ $\bar{1}$	(M653695)16	M10463440 · M-11
$\bar{1}$ 0 0 $\bar{1}$	(M10463429)16	M167414864 · M-9
$\bar{1}$ $\bar{1}$ 0 $\bar{1}$	(M167414855)16	M2678637680 · M-13 = M_2678637667

G. Canonical Recoding:

$\bar{1}$

10 0111111101010001100010001100011
10 100000101010010100010010100101

CASE d=1:

1 → 2 → 4 → 5 → 10 → 20 → 40 → 80 → 160 → 320 → 319 → 638 → 1276 → 1277 →
2554 → 5108 → 5109 → 10218 → 20436 → 40872 → 40873 → 81746 → 163492 →
163491 → 326982 → 653964 → 1307928 → 2615856 → 2615857 → 5231714 →
10463428 → 20926856 → 20926857 → 41853714 → 83707428 → 83707427 →

167414854 → 334829708 → 669659416 → 669659417 → 1339318834 → 2678637668 → 2678637667

Length = **43**

CASE d=2:

8 → 16 → 40 → 160 → 640 → 638 → 2552 → 2554 → 10216 → 10218 → 40872 → 40873 → 163492 → 163491 → 653964 → 2615856 → 2615857 → 10463428 → 41853712 → 41853714 → 167414856 → 167414854 → 669659416 → 669659417 → 2678637668 → 2678637667

Length = **29**

CASE d = 3:

2 → 16 → 20 → 160 → 1280 → 1277 → 10216 → 10218 → 81744 → 81746 → 653968 → 653964 → 5231712 → 5231714 → 41853712 → 334829712 → 334829708 → 2678637664 → 2678637667

Length = **22**

CASE d = 4:

10*16 → 160 → 2560 → 2554 → 40864 → 40855 → 653968 → 653964 → 10463424 → 10463428 → 167414848 → 167414854 → 2678637664 → 2678637667

Length = **19**

2) Illustrate the steps of the standard multiplication algorithm for computing $c=a*b=215*348$.

$$a * b = 215 * 348$$

i	j	Step	(C, S)	Partial t
0	0	$t_0 + a_0 b_0 + C$ $0 + 5 * 8 + 0$	$(0, _)$ $(4, 0)$	000000 000000
	1	$t_1 + a_1 b_0 + C$ $0 + 1.8 + 4$	$(1, 2)$	000020
	2	$t_2 + a_2 b_0 + C$ $0 + 2 * 8 + 1$	$(1, 7)$	000720
				001720
1	0	$t_1 + a_0 b_1 + C$ $2 + 5 * 4 + 0$	$(0, _)$ $(2, 2)$	001720
	1	$t_2 + a_1 b_1 + C$ $7 + 1 * 4 + 2$	$(1, 3)$	001320

2		$t_3 + a_2 b_1 + C$ $1+2 * 4+1$	(1, 0)	000320
				010320
2	0	$t_2 + a_0 b_2 + C$ $3+5 * 3+0$	(0, _) (1, 8)	010820
1		$t_3 + a_1 b_2 + C$ $0+1 * 3+1$	(0, 4)	014820
2		$t_4 + a_2 b_2 + C$ $1+2 * 3+0$	(0, 7)	074820
				074820

Answer: **074820**

3) Illustrate the steps of the standard squaring algorithm for computing $c=a*a=215*215$.

i	j	step	(C,S)	partial t
0	0	$t_0 + a_0 * a_0$ $0+5*5$	(0,_) (2,5)	000005
	1	$t_1 + 2 * a_1 * a_0 + C$ $0+2*1*5+2$	(1,2)	000025
	2	$t_2 + 2 * a_2 * a_0 + C$ $0+2*2*5+1$	(2,1)	000125
				002125
1		$t_2 + a_1 * a_1$ $1+1*1+0$	(0,_) (0,2)	002225
	2	$t_3 + 2 * a_1 * a_2 + C$ $2+2*1*2+0$	(0,6)	006225
2		$t_4 + a_2 * a_2$ $0+2*2$	(0,_) (0,4)	046225

Answer: 46225

4) Illustrate the steps of the restoring division algorithm for computing $R=243 \bmod 13$.

$t = 243$ (1111 0011)

$n = 13$ (1101)

R_0	1111 0011	t
n	1101	Subtract

+	0010	Positive rem.
	0010 0011	Not restore
$n/2$	110 1	

-	100 1	Negative rem.
R_1	0010 0011	Restore
$n/2$	11 01	

-	1 01	Negative rem.
R_2	0010 0011	Restore
$n/2$	1 101	

+	100	Positive rem.
---	-----	---------------

R_3 **1001** Final rem. \rightarrow Answer.

5) Illustrate the steps of the nonrestoring division algorithm for computing $R=243 \bmod 13$.

R_0	1111 0011	t
n	1101 0000	subtract

R_1	0010 0011	Positive rem.
$n/2$	0110 1000	Subtract

R_2	1011 1011	negative rem.
$n/2$	0011 0100	Add

R_3	1110 1111	negative rem.
$n/2$	0001 1010	Add

R 0000 **1001** Final Rem. \rightarrow Answer.

6) Let $n=29$, $e=23$, and $M=10$. Compute $M^e \pmod n$ using the binary method of exponentiation and the Montgomery multiplication where $r=32$. Show the steps of the binary method, and illustrate at least two Montgomery multiplications.

Computation of $10^{23} \pmod{29}$

$$r = 2^k = 32. \text{ Since}$$

$$32 * 10 - 29 * n' = 1$$

We have $n' = 11$.

$$M = 10$$

$$C = 1$$

$$M' = M * r \pmod n = 10 * 32 \pmod{29} = 1$$

$$C' = C * r \pmod n = 1 * 32 \pmod{29} = 3$$

Thus, $C' = 3$ and $M' = 1$

e in binary form = 10111

The loop goes from $i = 4$ to 0

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

Step 7: $C = \text{MonPro}(4, 1) = 11$

$x = 11$ (Ans)

$$\text{MonPro}(3, 3) = 3$$

$$t = 3 * 3 = 9$$

$$m = (9 * 11) \pmod{32} = 3$$

$$u = (9 + 3 * 29) / 32 = 3$$

$$= 3$$

$$\text{MonPro}(1, 3) = 1$$

$$t = 1 * 3 = 3$$

$$m = (3 * 11) \pmod{32} = 1$$

$$u = (3 + 29) / 32 = 1$$

$$\text{MonPro}(1, 1) = 10$$

$$t = 1 * 1 = 1$$

$$m = (1 * 11) \pmod{32} = 11$$

$$u = (1 + 11 \cdot 29) / 32 = 10$$

$$\text{MonPro}(10, 10) = 14$$

$$t = 10 \cdot 10 = 100$$

$$m = (100 \cdot 11) \bmod 32 = 12$$

$$u = (100 + 12 \cdot 29) / 32 = 14$$

$$\text{MonPro}(1, 14) = 24$$

$$t = 1 \cdot 14 = 14$$

$$m = (14 \cdot 11) \bmod 32 = 26$$

$$u = (14 + 26 \cdot 29) / 32 = 24$$

$$\text{MonPro}(24, 24) = 18$$

$$t = 24 \cdot 24 = 576$$

$$m = (576 \cdot 11) \bmod 32 = 0$$

$$u = (576 + 0 \cdot 29) / 32 = 18$$

$$\text{MonPro}(1, 18) = 6$$

$$t = 1 \cdot 18 = 18$$

$$m = (18 \cdot 11) \bmod 32 = 6$$

$$u = (18 + 6 \cdot 29) / 32 = 6$$

$$\text{MonPro}(6, 6) = 12$$

$$t = 6 \cdot 6 = 36$$

$$m = (36 \cdot 11) \bmod 32 = 12$$

$$u = (36 + 12 \cdot 29) / 32 = 12$$

$$\text{MonPro}(1, 12) = 4$$

$$t = 1 \cdot 12 = 12$$

$$m = (12 \cdot 11) \bmod 32 = 4$$

$$u = (12 + 4 \cdot 29) / 32 = 4$$

7) Let $r=32$, $n=25$, $a=13$, and $b=15$. Compute $c=a \cdot b \cdot r^{-1} \bmod n$ using the binary add-shift Montgomery multiplication algorithm. Illustrate the steps and give all temporary results.

$$a = 1101 \quad b = 1111 \quad r = 32 = 2^5 \quad k = 5 \quad n = 11001$$

Compute $a \cdot b \cdot 2^{-k} \bmod n$

$$u = (a_{k-1}^{2-1} + a_{k-2}^{2-2} + \dots + a_0^{2-k}) \cdot b \bmod n$$

$$u = u + a_i \cdot b$$

$$i \quad u = u + a_i \cdot b$$

$$\text{odd-} u = u + n$$

$$\text{even-} u = u/2$$

0	$0000 + 1*1111 = 1111$	101000	10100
1	$10100 + 0*1111 = 10100$		1010
2	$1010 + 1*1111 = 11001$	110010	11001
3	$11001 + 1*1111 = 101000$		10100
4	$10100 + 0*1111 = 10100$		1010

$$a.b.r^{-1} \bmod n = 13.15.32^{-1} \bmod 32 = \mathbf{10 (1010_2)}$$

$$a = 13, b = 15, n = 25, r = 32$$

Method:

$$\begin{aligned} \text{Computation of } n' \\ n' &= 32 * 18 - 1 / 25 \\ n' &= 23 \end{aligned}$$

$$\text{MonPro}(a, b) = a * b * r^{-1} \bmod n$$

$$t = a * b = 13 * 15 = 195$$

$$\begin{aligned} m &= t * n' \bmod r \\ m &= 195 * 23 \bmod 32 = 5 \end{aligned}$$

$$\begin{aligned} u &= (t + m * n) / r \\ u &= (195 + 5 * 25) / 32 = 10 \\ c &= a * b * r^{-1} \bmod n \\ &= \mathbf{10 \text{ Ans}} \end{aligned}$$
