Cryptology Design Fundamentals

Grundlagen des kryptographischen Systementwurfs

Module ID: ET-IDA-048

Tutorial-02-2
Supplementary-Experimental Analysis

Mathematical Background:
Groups, Rings, Finite Fields (GF)

05.01.2015, v5
Prepared by : Tianqing Su

Prof. W. Adi

Tutorials extensions for lecture 3

Rings, Fields, Groups

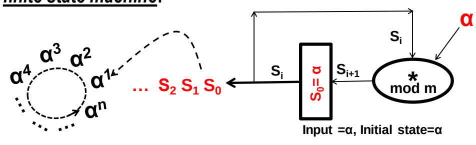
Includes full analysis :

$For\ \ GF(41),\ Z_{56},\ \ Z_{2^n}\ (\text{for } n=5)$

$And\ \ Z_{2^n+1}(\text{for } n=5)\ ,\ Z_{2^n-1}\ (\text{for } n=4)$

Objectives of this extended analysis

Engineering is interested in the behaviour of this *finite state machine*:



What is the deterministic size n of this loop?
That is the period of the element α (element's order or period/sequence length)

Problem 1: Elements of Z_{41} = GF(41)

1. Which additive orders are possible in GF(41)
2. How many invertible element under multiplication do exist in GF(41) (number of units in GF(41))?
3. Which multiplicative orders are possible in GF(41)
4. Compute the number of elements from each order
5. Compute the order of all elements in GF(41) using the primitive element 7

Solution 1:

1. Additive group = (0,1,2, ..., 40)
   The smallest positive solution of the congruence ax = 0 (mod n) is called the additive order of a modulo n
   The possible additive orders in GF(41) are the divisors of order of the additive group, **namely 1, 41**
   The additive order of element b in GF(41):
   for $b \neq 0$ **=> order of b is 41**
   for $b = 0$ **=> order of b is 1**
2. Number of invertible elements (units) is Euler function **$\phi(41)$ = 41-1 = 40**
3. The possible multiplicative orders in GF(41) are the divisors of $\phi(41)$**=40= 2.2.2.5** , **namely 1, 2, 4, 5, 8, 10, 20,40**
4. Number of elements with order 1 is **$\phi(1) = 1$**
   Number of elements with order 2 is **$\phi(2) = (2-1) = 1$**
   Number of elements with order 4 is **$\phi(4) = 4\ (1-1/2) = 2$**
   Number of elements with order 5 is **$\phi(5) = (5-1)= 4$**
   Number of elements with order 8 is **$\phi(8) = \phi(8) = \phi(2^3)= 8\ (1-1/2) = 4$**
   Number of elements with order 10 is **$\phi(10) = \phi(2x5) = (2-1)(5-1) = 4$**
   Number of elements with order 20 is **$\phi(20) = \phi(2x2x5) = 20(1-1/2)(1-1/5) = 8$**
   Number of elements with order 40 is **$\phi(40) = \phi(2x2x2x5)= 40(1-1/2)(1-1/5) = 16$**

Solution 1:

5. Order of 7: $7^1 = 7 \neq 1$, $7^2 = 8 \neq 1$, $7^4 = 8^2 = 23 \neq 1$, $7^5 = 7x(23)=38 \neq 1$, $7^8 = 23^2 = 37$, $7^{10} = 38^2 = 9 \neq 1$, $7^{20} = 9^2 = 40$
   => order of 7 is 40, 7 is a primitive element, which can generate the whole group.
   If the order of α is k then Ord (α^i) = k / gcd (i,k).

   By selecting i=40 we get gcd(40,i)=40. Ord (7^i) = 40 / gcd (i,40)= 40/ 40= 1
   => 7^{40} **or 1 are 1 element having order 1**
   By selecting i=20 we get gcd(40,i)=20. Ord (7^i) = 40 / gcd (i,40)= 40/ 20= 2
   => 7^{20} **or 40 are 1 element having order 2**
   By selecting i=10,30 we get gcd(40,i)=10. . Ord (7^i) = 40 / gcd (i,40)= 40/ 10= 4
   => 7^{10} , 7^{30} **or 9 , 32 are 2 elements having order 4**
   By selecting i=8, 16, 24, 32 we get gcd(40,i)=8 . Ord (7^i) = 40 / gcd (i,40)= 40/ 8= 5
   => 7^8, 7^{16} , 7^{24} , 7^{32} **or 37 , 16 , 18 , 10 are 4 elements having order 5**
   By selecting i= 5, 15, 25, 35 we get gcd(40,i)=5. . Ord (7^i) = 40 / gcd (i,40)= 40/ 5= 8
   => 7^5, 7^{15} , 7^{25} , 7^{35} **or 38 , 14 , 3 , 27 are 4 elements having order 8**
   By selecting i=4, 12, 28, 36 we get gcd(40,i)=4. . Ord (7^i) = 40 / gcd (i,40)= 40/ 4= 10
   => 7^4, 7^{12} , 7^{28} , 7^{36} **or 23 , 31 , 4 , 25 are 4 elements having order 10**
   By selecting i=2, 6, 14, 18, 22, 26, 34, 38 we get gcd(40,i)=2. . Ord (7^i) = 40 / gcd (i,40)= 40/ 2= 20
   => 7^2, 7^6 , 7^{14}, 7^{18}, 7^{22} , 7^{26} , 7^{34}, 7^{38} **or 8 , 20 , 2 , 5 , 33 , 21 , 39 , 36 are 8 elements having order 20**
   By selecting i= 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39
   we get gcd(40,i)=1. . Ord (7^i) = 40 / gcd (i,40)= 40/ 1= 40
   => 7^1, 7^3 , 7^7 , 7^9, 7^{11} , 7^{13} , 7^{17}, 7^{19} , 7^{21} , 7^{23}, 7^{27} , 7^{29} , 7^{31} , 7^{33} , 7^{37}, 7^{39} **or**
   7 , 15 , 17 , 13 , 22 , 12 , 30 , 35 , 34 , 26 , 24 , 28 , 19 , 29 , 11 , 6 are 16 elements having order 40

Multiplicative orders of all exponents of the primitive element a=7 in the ring Z_{56}

i	7^(i)	gcd(40,i)	Ord(7^i)=40/gcd(40,i)	i	7^(i)	gcd(40,i)	Ord(7^i)=40/gcd(40,i)
1	7	1	40	21	34	1	40
2	8	2	20	22	33	2	20
3	15	1	40	23	26	1	40
4	23	4	10	24	18	8	5
5	38	5	8	25	3	5	8
6	20	2	20	26	21	2	20
7	17	1	40	27	24	1	40
8	37	8	5	28	4	4	10
9	13	1	40	29	28	1	40
10	9	10	4	30	32	10	4
11	22	1	40	31	19	1	40
12	31	4	10	32	10	8	5
13	12	1	40	33	29	1	40
14	2	2	20	34	39	2	20
15	14	5	8	35	27	5	8
16	16	8	5	36	25	4	10
17	30	1	40	37	11	1	40
18	5	2	20	38	36	2	20
19	35	1	40	39	6	1	40
20	40	20	2	40	1	40	1

Problem 2: Elements of the ring Z_{56}

1. How many invertible element under multiplication do exist in Z_{56} (number of units in Z_{56}) ?
2. Which multiplicative orders are possible in Z^*_{56}
3. Compute the order of the elements of Z^*_{56}
4. Compute the order of many non-unit elements

Solution 2:

1. Number of invertible elements (units) is Euler function **$\phi(56) = \phi(2^3 x7) = 56(1-1/2)(1-1/7) = 24$**
   The 24 units in Z_{56} are: **u=1,3,5,9,11,13,15,17,19,23,25,27,29,31,33,37,39,41,43,45,47,51,53,55** (gcd (56,u)=1)
2. The possible orders in Z_{56} are the divisors of $\lambda(56)$ = lcm [$\lambda(2^3)$, $\lambda(7)$] =lcm (2,6)= 2x6/gcd(2,6)=**6**
   => the divisors of 6 are **1, 2, 3, 6**
3. Order of 3: $3^1 = 3 \neq 1$, $3^2 = 6 \neq 1$, $3^3 = 27 \neq 1$ => **order of 3 is 6**
   Order of 5: $5^1 = 5 \neq 1$, $5^2 = 25 \neq 1$, $5^3 = 13 \neq 1$ => **order of 5 is 6**
   Order of 9: $9^1 = 9 \neq 1$, $9^2 = 25 \neq 1$, $9^3 = 25x9 = 1$ => **order of 9 is 3**
   Order of 11: $11^1 = 11 \neq 1$, $11^2 = 9 \neq 1$, $11^3 = 9x11 = 43 \neq 1$ => **order of 11 is 6**
   Order of 13: $13^1 = 13 \neq 1$, $13^2 = 1$ => **order of 13 is 2**
   Order of 15: $15^1 = 15 \neq 1$, $15^2 = 1$ => **order of 15 is 2**
   Order of 17: $17^1 = 17 \neq 1$, $17^2 = 9 \neq 1$, $17^3 = 17x9 = 41 \neq 1$ => **order of 17 is 6**
   Order of 19: $19^1 = 19 \neq 1$, $19^2 = 25 \neq 1$, $19^3 = 25x19 = 27 \neq 1$ => **order of 19 is 6**
   Order of 23: $23^1 = 23 \neq 1$, $23^2 = 25 \neq 1$, $23^3 = 25x23 = 15 \neq 1$ => **order of 23 is 6**
   Order of 25: $25^1 = 25 \neq 1$, $25^2 = 9 \neq 1$, $25^3 = 9x25 = 1$ => **order of 25 is 3**
   Order of 27: $27^1 = 27 \neq 1$, $27^2 = 1$ => **order of 27 is 2**
   Order of 29: $29^1 = 29 \neq 1$, $29^2 = 1$ => **order of 29 is 2**
   Order of 31: $31^1 = 31 \neq 1$, $31^2 = 9 \neq 1$, $31^3 = 9x31 = 55 \neq 1$ => **order of 31 is 6**

Solution 2:

3. Order of 33: $33^1 = 33 \neq 1$, $33^2 = 25 \neq 1$, $33^3 = 25x33 = 41 \neq 1$ => **order of 33 is 6**
   Order of 37: $37^1 = 37 \neq 1$, $37^2 = 25 \neq 1$, $37^3 = 25x37 = 29 \neq 1$ => **order of 37 is 6**
   Order of 39: $39^1 = 39 \neq 1$, $39^2 = 9 \neq 1$, $39^3 = 9x39 = 15 \neq 1$ => **order of 39 is 6**
   Order of 41: $41^1 = 41 \neq 1$, $41^2 = 1$ => **order of 41 is 2**
   Order of 43: $43^1 = 43 \neq 1$, $43^2 = 1$ => **order of 43 is 2**
   Order of 45: $45^1 = 45 \neq 1$, $45^2 = 9 \neq 1$, $45^3 = 9x45 = 13 \neq 1$ => **order of 45 is 6**
   Order of 47: $47^1 = 47 \neq 1$, $47^2 = 25$, $47^3 = 25x47 = 55 \neq 1$ => **order of 47 is 6**
   Order of 51: $51^1 = 51 \neq 1$, $51^2 = 25 \neq 1$, $51^3 = 25x51 = 43 \neq 1$ => **order of 51 is 6**
   Order of 53: $53^1 = 53 \neq 1$, $53^2 = 9$, $53^3 = 9x53 = 29 \neq 1$ => **order of 53 is 6**
   Order of 55: $55^1 = 55 \neq 1$, $55^2 = 1$ => **order of 55 is 2**

alternativ:

Order of 3: $3^1 = 3 \neq 1$, $3^2 = 6 \neq 1$, $3^3 = 27 \neq 1$ => order of 3 is 6
If order α=k, then ord (α^i) = k iff gcd(k,i) =1.
By selecting i=1,5 we get gcd(6,i)=1 => **3^1 3^5 or 3 ,19 having order 6**
Order of 5: $5^1 = 5 \neq 1$, $5^2 = 25 \neq 1$, $5^3 = 13 \neq 1$ => order of 5 is 6
By selecting i=1,5 we get gcd(6,i)=1. => **5^1 5^5 or 5 , 45 having order 6**
Order of 9: $9^1 = 9 \neq 1$, $9^2 = 25 \neq 1$, $9^3 = 25x9 = 1$ => order of 9 is 3
By selecting i=1,2 we get gcd(3,i)=1. => **9^1 9^2 or 9 , 25 having order 3**
Order of 11: $11^1 = 11 \neq 1$, $11^2 = 9 \neq 1$, $11^3 = 9x11 = 43 \neq 1$ => order of 11 is 6
By selecting i=1,5 we get gcd(6,i)=1. => **11^1 11^5 or 11 , 51 having order 6**
Etc …..

Multiplicative orders of all units in the ring Z_{56}

n	n^1	n^2	n^3	n^6	Ord(n)
1	1				1
3	3	9	27	1	6
5	5	25	13	1	6
9	9	25	1		3
11	11	9	43	1	6
13	13	1			2
15	15	1			2
17	17	9	41	1	6
19	19	25	27	1	6
23	23	25	15	1	6
25	25	9	1		3
27	27	1			2
29	29	1			2
31	31	9	55	1	6
33	33	25	41	1	6
37	37	25	29	1	6
39	39	9	15	1	6
41	41	1			2
43	43	1			2
45	45	9	13	1	6
47	47	25	55	1	6
51	51	25	43	1	6
53	53	9	29	1	6
55	55	1			2

Solution 2:

4. **Cycle structures of non-units**
   Element 2 is not invertible. Exponents of 2: $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32$,
   $2^6 = 8$, $2^7 = 16$, $2^8 = 32$,
   $2^9 = 8$, $2^{10} = 16$, $2^{11} = 32$
   ……
   $2^{54} = 8$, $2^{55} = 16$

Notice: **order 2 as a non unit is by definition = ∞**

Cycle structure of the exponents of 2:
2 → 4 → 8 → 16
32

Element 4 is not invertible. Exponents of 4: $4^1 = 4$, $4^2 = 16$, $4^3 = 8$, $4^4 = 32$,
$4^5 = 16$, $4^6 = 8$, $4^7 = 32$,
$4^8 = 16$, $4^9 = 8$, $4^{10} = 32$
……
$4^{53} = 16$, $4^{54} = 8$, $4^{55} = 32$

Singular sequence (no pure looping)

Notice: **order 4 as a non unit is by definition = ∞**

Cycle structure of the exponents of 4:
4 → 16 → 8
32

The following table shows the cycle structure of all non-units in Z_{56}
Notice: the involved cycles have a length which divides $\lambda(56)$ = **6**

Cycle structure of all non-units in the ring Z_{56}

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	48	49	50	51	52	53	54
n	n^1	n^2	n^3	n^4	n^5	n^6	n^7	n^8	n^9	n^10	n^11	n^12	n^13	n^14	n^15~47	n^48	n^49	n^50	n^51	n^52	n^53	n^54
2	2	4	8	16	32	8	16	32	8	16	32				cycle structure	8	16	32	8	16	32	8
4	4	16	8	32	16	8	32	16	8	32					cycle structure	8	32	16	8	32	16	8
6	6	36	48	8	48	8	48	8							cycle structure	8	48	8	48	8	48	8
7	7	49	7	49	7	49									cycle structure	49	7	49	7	49	7	49
8	8	8	8												cycle structure	8	8	8	8	8	8	8
10	10	44	48	32	40	8	24	16	48	32	40	8	24	16	cycle structure	8	24	16	48	32	40	8
12	12	32	48	16	24	8	40	32	48	16	24	8	40	32	cycle structure	8	40	32	48	16	24	8
14	14	28	0	0	0										cycle structure	0	0	0	0	0	0	0
16	16	32	8	16	32	8									cycle structure	8	16	32	8	16	32	8
18	18	44	8	32	16	8	32	16	8	32	16				cycle structure	8	32	16	8	32	16	8
20	20	8	48	8	48	8	48								cycle structure	8	48	8	48	8	48	8
21	21	49	21	49	21	49									cycle structure	49	21	49	21	49	21	49
22	22	36	8	8	8										cycle structure	8	8	8	8	8	8	8
24	24	16	48	32	40	8	24	16	48	32	40	8	24		cycle structure	8	24	16	48	32	40	8
26	26	4	48	16	24	8	40	32	48	16	24	8	40	32	cycle structure	8	40	32	48	16	24	8
28	28	0	0	0						0					cycle structure	0	0	0	0	0	0	0
30	30	4	8	16	32	8	16	32	8	16	32				cycle structure	8	16	32	8	16	32	8
32	32	16	8	32	16	8	32	16	8						cycle structure	8	32	16	8	32	16	8
34	34	36	48	8	48	8	48	8							cycle structure	8	48	8	48	8	48	8
35	35	49	35	49	35	49									cycle structure	49	35	49	35	49	35	49
36	36	8	8	8											cycle structure	8	8	8	8	8	8	8
38	38	44	48	32	40	8	24	16	48	32	40	8	24	16	cycle structure	8	24	16	48	32	40	8
40	40	32	48	16	24	8	40	32	48	16	24	8	40	32	cycle structure	8	40	32	48	16	24	8
42	42	28	0	0	0	0									cycle structure	0	0	0	0	0	0	0
44	44	32	8	16	32	8	16	32	8	16					cycle structure	8	16	32	8	16	32	8
46	46	44	8	32	16	8	32	16	8	32	16				cycle structure	8	32	16	8	32	16	8
48	48	8	48	8	48	8									cycle structure	8	48	8	48	8	48	8
49	49	49	49												cycle structure	49	49	49	49	49	49	49
50	50	36	8	8	8										cycle structure	8	8	8	8	8	8	8

Problem 3: Elements of the ring Z_{32}

1. How many invertible element under multiplication do exist in Z_{32} (number of units in Z_{32}) ?
2. Which multiplicative orders are possible in Z^*_{32}
3. Compute the order of the elements of Z^*_{32}
4. Compute the order of many non-unit elements

Solution 3:

1. Number of invertible elements (units) is Euler function **$\phi(32) = \phi(2^5) = 32(1-1/2) = 16$**
   The 16 units in Z_{32} are: **u=1,3,5,7,9,11,13,15,17,19,21,23,25,27,29,31** (gcd (32,u)=1)
2. The possible orders in Z_{32} are the divisors of $\lambda(32) = \lambda(2^5) = 2^3 =$ **8**
   => the divisors of 8 are **1, 2, 4, 8**
3. Order of 3: $3^1 = 3 \neq 1$, $3^2 = 9 \neq 1$, $3^4 = 9^2 = 17 \neq 1$ => **order of 3 is 8**
   Order of 5: $5^1 = 5 \neq 1$, $5^2 = 25 \neq 1$, $5^4 = 25^2 = 17 \neq 1$ => **order of 5 is 8**
   Order of 7: $7^1 = 7 \neq 1$, $7^2 = 17 \neq 1$, $7^4 = 17^2 = 1$ => **order of 7 is 4**
   Order of 9: $9^1 = 9 \neq 1$, $9^2 = 17 \neq 1$, $9^4 = 1$ => **order of 9 is 4**
   Order of 11: $11^1 = 11 \neq 1$, $11^2 = 25 \neq 1$, $11^4 = 17 \neq 1$ => **order of 11 is 8**
   Order of 13: $13^1 = 13 \neq 1$, $13^2 = 9 \neq 1$, $13^4 = 17 \neq 1$ => **order of 13 is 8**
   Order of 15: $15^1 = 15 \neq 1$, $15^2 = 1$ => **order of 15 is 2**
   Order of 17: $17^1 = 17 \neq 1$, $17^2 = 1$ => **order of 17 is 2**
   Order of 19: $19^1 = 19 \neq 1$, $19^2 = 9 \neq 1$, $19^4 = 17 \neq 1$ => **order of 19 is 8**
   Order of 21: $21^1 = 21 \neq 1$, $21^2 = 25 \neq 1$, $21^4 = 17 \neq 1$ => **order of 21 is 8**
   Order of 23: $23^1 = 23 \neq 1$, $23^2 = 17 \neq 1$, $23^4 = 1$ => **order of 23 is 4**
   Order of 25: $25^1 = 25 \neq 1$, $25^2 = 25 \neq 1$, $25^4 = 1$ => **order of 25 is 4**

Solution 3:

3. Order of 27: $27^1 = 27 \neq 1$, $27^2 = 25 \neq 1$, $27^4 = 17 \neq 1$ => **order of 27 is 8**
   Order of 29: $29^1 = 29 \neq 1$, $29^2 = 9 \neq 1$, $29^4 = 17 \neq 1$ => **order of 29 is 8**
   Order of 31: $31^1 = 31 \neq 1$, $31^2 = 1$ => **order of 31 is 2**

alternativ:

Order of 3: $3^1 = 3 \neq 1$, $3^2 = 9 \neq 1$, $3^4 = 9^2 = 17 \neq 1$ => order of 3 is 8
If order α=k, then ord (α^i) = k iff gcd(k,i) =1.
By selecting i=1,3,5,7 we get gcd(8,i)=1, Ord (3^i) = 8 / gcd (i,8)= 8
=> 3^1 3^3 3^5 3^7 or 3, 27, 19, 11 having order 8
Order of 5: $5^1 = 5 \neq 1$, $5^2 = 25 \neq 1$, $5^4 = 25^2 = 17 \neq 1$ => order of 5 is 8
By selecting i=1,3,5,7 we get gcd(8,i)=1.
=> 5^1 5^3 5^5 5^7 or 5 , 29, 21, 13 having order 8
Order of 7: $7^1 = 7 \neq 1$, $7^2 = 17 \neq 1$, $7^4 = 17^2 = 1$ => order of 7 is 4
By selecting i=1,3 we get gcd(4,i)=1.
=> 7^1 7^3 or 9 , 23 having order 4
Order of 15: $15^1 = 15 \neq 1$, $15^2 = 1$ => **order of 15 is 2**
Etc …..

Multiplicative orders of all units in the ring Z_{32}

n	n^1	n^2	n^4	n^8	Ord(n)
1	1				1
3	3	9	17	1	8
5	5	25	17	1	8
7	7	17	1		4
9	9	17	1		4
11	11	25	17	1	8
13	13	9	17	1	8
15	15	1			2
17	17	1			2
19	19	9	17	1	8
21	21	25	17	1	8
23	23	17	1		4
25	25	17	1		4
27	27	25	17	1	8
29	29	9	17	1	8
31	31	1			2

Solution 3:

4. Element 2 is not invertible. Exponents of 2: $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 0$, $2^6 = 0$, $2^7 = 0$, $2^8 = 0$,
……
$2^{30} = 0$, $2^{31} = 0$

Notice: **order 2 as a non unit is by definition = ∞**

Element 4 is not invertible. Exponents of 4: $4^1 = 4$, $4^2 = 16$, $4^3 = 0$, $4^4 = 0$, $4^5 = 0$, $4^6 = 0$, $4^7 = 0$, $4^8 = 0$,
……
$4^{30} = 0$, $4^{31} = 0$

Notice: **order 4 as a non unit is by definition = ∞**

Element 30 is not invertible. Exponents of 30: $30^1 = 30$, $30^2 = 4$, $30^3 = 24$, $30^4 = 16$, $30^5 = 0$, $30^6 = 0$, $30^7 = 0$,
……
$30^{30} = 0$, $30^{31} = 0$

Notice: **order 30 as a non unit is by definition = ∞**

Cycle structure of all non-units in the ring Z_{32}

	1	2	3	4	5	6	7	8	9	10	11	12	13	15	16-31
n	n^1	n^2	n^3	n^4	n^5	n^6	n^7	n^8	n^9	n^10	n^11	n^12	n^13	n^15	n^16-n^31
2	2	4	8	16	0	0	0	0	0	0	0	0	0	0	0
4	4	16	0	0	0	0	0	0	0	0	0	0	0	0	0
6	6	4	24	16	0	0	0	0	0	0	0	0	0	0	0
8	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	10	4	8	16	0	0	0	0	0	0	0	0	0	0	0
12	12	16	0	0	0	0	0	0	0	0	0	0	0	0	0
14	14	4	24	16	0	0	0	0	0	0	0	0	0	0	0
16	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	18	4	8	16	0	0	0	0	0	0	0	0	0	0	0
20	20	16	0	0	0	0	0	0	0	0	0	0	0	0	0
22	22	4	24	16	0	0	0	0	0	0	0	0	0	0	0
24	24	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	26	4	8	16	0	0	0	0	0	0	0	0	0	0	0
28	28	16	0	0	0	0	0	0	0	0	0	0	0	0	0
30	30	4	24	16	0	0	0	0	0	0	0	0	0	0	0

Problem 4: Elements of Z_n Where n is not a prime and $n=2^t+1$ or $n=2^t-1$ for several values of t.

1. How many invertible element under multiplication do exist in Z_n (number of units in Z_n) ?
2. Which multiplicative orders are possible in Z^*_n
3. Compute the order of the elements of Z^*_n
4. Compute the order of many non-unit elements

Solution 4:

For t=5, $n = 2^t + 1 = 33$

1. Number of invertible elements (units) is Euler function **$\phi(33) = \phi(3x11) = 2x10 = 20$**
2. The 20 units in Z_{33} are: **u=1,2,4,5,7,8,10,13,14,16,17,19,20,23,25,26,28,29,31,32** (gcd (33,u)=1)
   The possible multiplicative orders in Z^*_{33} are the divisors of $\lambda(33)$= lcm [$\lambda(3)$, $\lambda(11)$]= lcm(2,10)=10
   namely 1, 2, 5, 10
3. Order of 2: $2^1 = 2 \neq 1$, $2^2 = 4 \neq 1$, $2^5 = 32 \neq 1$ => **order of 2 is 10**
   Order of 4: $4^1 = 4 \neq 1$, $4^2 = 16 \neq 1$, $4^5 = 1$ => **order of 4 is 5**
   Order of 5: $5^1 = 5 \neq 1$, $5^2 = 25 \neq 1$, $5^5 = 23 \neq 1$ => **order of 5 is 10**
   Order of 7: $7^1 = 7 \neq 1$, $7^2 = 16 \neq 1$, $7^5 = 10 \neq 1$ => **order of 7 is 10**
   Order of 8: $8^1 = 8 \neq 1$, $8^2 = 31 \neq 1$, $8^5 = 32 \neq 1$ => **order of 8 is 10**
   Order of 10: $10^1 = 10 \neq 1$, $10^2 = 1$ => **order of 10 is 2**
   Order of 13: $13^1 = 13 \neq 1$, $13^2 = 4 \neq 1$, $13^5 = 10 \neq 1$ => **order of 13 is 10**
   Order of 14: $14^1 = 14 \neq 1$, $14^2 = 31 \neq 1$, $14^5 = 23 \neq 1$ => **order of 14 is 10**
   Order of 16: $16^1 = 16 \neq 1$, $16^2 = 25 \neq 1$, $16^5 = 1$ => **order of 16 is 5**

Solution 4:

3. Order of 17: $17^1 = 17 \neq 1$, $17^2 = 25 \neq 1$, $17^5 = 32 \neq 1$ => **order of 17 is 10**
   Order of 19: $19^1 = 19 \neq 1$, $19^2 = 31 \neq 1$, $19^5 = 10 \neq 1$ => **order of 19 is 10**
   Order of 20: $20^1 = 20 \neq 1$, $20^2 = 4 \neq 1$, $20^5 = 23 \neq 1$, => **order of 20 is 10**
   Order of 23: $23^1 = 23 \neq 1$, $23^2 = 1$ => **order of 23 is 2**
   Order of 25: $25^1 = 25 \neq 1$, $25^2 = 31 \neq 1$, $25^5 = 1$ => **order of 25 is 5**
   Order of 26: $26^1 = 26 \neq 1$, $26^2 = 16 \neq 1$, $26^5 = 23 \neq 1$ => **order of 26 is 10**
   Order of 28: $28^1 = 28 \neq 1$, $28^2 = 25 \neq 1$, $28^5 = 10 \neq 1$ => **order of 28 is 10**
   Order of 29: $29^1 = 29 \neq 1$, $29^2 = 16 \neq 1$, $29^5 = 32 \neq 1$ => **order of 29 is 10**
   Order of 31: $31^1 = 31 \neq 1$, $31^2 = 4 \neq 1$, $31^5 = 1$ => **order of 31 is 5**
   Order of 32: $32^1 = 32 \neq 1$, $32^2 = 1$ => **order of 32 is 2**

4. **Cycle structure of all non-units in the ring Z_{33}**

3	3	9	27	15	12	3	9	27	15	12										
6	6	3	18	9	21	27	30	15	24	12	6	3	18	9	21	27	30	15	24	12
9	9	15	3	27	12	9	15	3	27	12										
11	11	22	11	22																
12	12	12																		
15	15	27	9	3	12	15	27	9	3	12										
18	18	27	24	3	21	15	6	9	30	12	18	27	24	3	21	15	6	9	30	12
21	21	12	21	12																
22	22	22																		
24	24	15	30	27	21	9	18	3	6	12	24	15	30	27	21	9	18	3	6	12
27	27	3	15	9	12	27	3	15	9	12										
30	30	9	6	15	21	3	24	27	18	12	30	9	6	15	21	3	24	27	18	12

Solution 4:

For $t=4, n= n=2^t -1=15$

1. Number of invertible elements (units) is Euler function **$\phi(15) = \phi(3x5) = 2x4 = 8$**
2. The 8 units in Z_{15} are: **u=1,2,4,7,8,11,13,14** (gcd (15,u)=1)
   The possible multiplicative orders in Z^*_{15} are the divisors of $\lambda(15)$**=** lcm $[\lambda(3), \lambda(5)]$= lcm(2,4)=4
   namely 1, 2, 4
3. Order of 2: $2^1 = 2 \neq 1$, $2^2 = 4 \neq 1$ => order of 2 is 4
   By selecting i=1,3 we get gcd(4,i)=1 **=> 2^1 2^3 or 2 ,8 having order 4**
   Order of 4: $4^1 = 4 \neq 1$, $4^2 = 1$, **=> order of 4 is 2**
   Order of 7: $7^1 = 7 \neq 1$, $7^2 = 4 \neq 1$ => order of 7 is 4
   By selecting i=1,3 we get gcd(4,i)=1 **=> 7^1 7^3 or 7 ,13 having order 4**
   Order of 11: $11^1 = 11 \neq 1$, $11^2 = 1$ **=> order of 11 is 2**
   Order of 14: $14^1 = 14 \neq 1$, $14^2 = 1$ **=> order of 14 is 2**

4. **Cycle structure of all non-units in the ring Z_{15}**

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
n	n^1	n^2	n^3	n^4	n^5	n^6	n^7	n^8	n^9	n^10	n^11	n^12	n^13	n^14
3	3	9	12	6	3	9	12	6	3	9	12	6	3	9
5	5	10	5	10	5	10	5	10	5	10	5	10	5	10
9	9	6	9	6	9	6	9	6	9	6	9	6	9	6
10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
12	12	9	3	6	12	9	3	6	12	9	3	6	12	9

Problem 5: Elements of the ring Z_{113}

1. How many invertible element under multiplication do exist in Z_{113} (number of units in Z_{113}) ?
2. Which multiplicative orders are possible in Z^*_{113}
3. How many primitive elements under multiplication do exist in Z_{113}
4. Compute the order of the elements of Z^*_{113}

Solution 2:

1. Number of invertible elements (units) is Euler function **$\phi(113) =(113-1) = 112$**
   The 112 units in Z_{113} are: **u=1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17, …... 112** (gcd (113,u)=1)
2. The possible multiplicative orders in GF(113) are the divisors of $\phi(113)$**=112= 2.2.2.2.7** , **namely 1, 2, 4, 7, 8, 14, 16,28,56,112**
3. The number of primitive elements in a finite field *GF*(*n*) is **$\phi(n - 1) =\phi(112) = \phi(2^4 x7) =112(1-1/2)(1-1/7) = 48$**
4. Order of 2: $2^1 = 2 \neq 1$, $2^2 = 4 \neq 1$, $2^4 = 16 \neq 1$, $2^7 = 15 \neq 1$, $2^8 = 30 \neq 1$, $2^{14} = 112 \neq 1$ $2^{16} = 109 \neq 1$, $2^{28} = 1$
   => order of 2 is 28
   Order of 3: $3^1 = 3 \neq 1$, $3^2 = 9 \neq 1$, $3^4 = 81 \neq 1$, $3^7 = 40 \neq 1$, $3^8 = 7 \neq 1$, $3^{14} = 18 \neq 1$, $3^{16} = 49 \neq 1$, $3^{28} = 98 \neq 1$, $3^{56} = 112 \neq 1$
   => order of 3 is 112
   Order of 4: $4^1 = 4 \neq 1$, $4^2 = 16 \neq 1$, $4^4 = 30 \neq 1$, $4^7 = 112 \neq 1$, $4^8 = 109 \neq 1$, $4^{14} = 1 \neq 1$
   => order of 4 is 14
   Order of 5: $5^1 = 5 \neq 1$, $5^2 = 25 \neq 1$, $5^4 =60 \neq 1$, $5^7 = 42 \neq 1$, $5^8 = 97 \neq 1$, $5^{14} =69 \neq 1$, $5^{16} = 30 \neq 1$, $5^{28} = 15 \neq 1$, $5^{56} =112 \neq 1$
   => order of 5 is 112
   Etc …

Multiplicative orders of all units in the ring Z_{113}

n	n^1	n^2	n^4	n^7	n^8	n^14	n^16	n^28	n^56	n^112	Ord(n)
1	1	1	1	1	1	1	1	1			1
2	2	4	16	15	30	112	109	1			28
3	3	9	81	40	7	18	49	98	112	1	112
4	4	16	30	112	109	1					14
5	5	25	60	42	97	69	30	15	112	1	112
6	6	36	53	35	97	95	30	98	112	1	112
7	7	49	28	112	106	1					14
8	8	64	28	98	106	112	49	1			28
9	9	81	7	18	49	98	28	112	1		56
10	10	100	56	65	85	44	106	15	112	1	112
11	11	8	64	95	28	98	106	112	1		56
12	12	31	57	73	85	18	106	98	112	1	112
13	13	56	85	69	106	15	49	112	1		56
14	14	83	109	98	16	112	30	1			28
15	15	112	1								4
16	16	30	109	1							7
17	17	63	14	78	83	95	109	98	112	1	112
18	18	98	112	44	1						8
19	19	22	32	42	7	63	49	15	112	1	112
20	20	61	105	71	64	69	28	15	112	1	112
21	21	102	8	73	64	18	28	98	112	1	112
22	22	32	7	69	49	15	28	112	1		56
23	23	77	53	73	97	18	30	98	112	1	112
24	24	11	8	78	64	95	28	98	112	1	112
25	25	60	97	69	30	15	109	112	1		56
26	26	111	4	18	16	98	30	112	1		56
27	27	51	2	42	4	69	16	15	112	1	112
28	28	106	49	1							7
29	29	50	14	73	83	18	109	98	112	1	112
30	30	109	16	1							7
…...											
108	108	25	60	71	97	69	30	15	112	1	112
109	109	16	30	1							
110	110	9	81	73	7	18	49	98	96	1	112
111	111	4	16	98	30	112	109	1			28
112	112	1									2