Introduction to Cryptology

Tutorial-02-1
Mathematical Background:
Groups, Rings, Finite Fields (GF)

15.03.2023, v47

Summary: Ring of Integers modulo m Z_m

Euler Function $\phi(m)$ gives the number of invertible elements in Z_m

For $m = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_t^{e_t}$ $\longrightarrow$ $\phi(m) = m\,(1 - \frac{1}{P_1})\,(1 - \frac{1}{P_2}) \ldots\ldots$

For $m = p_1\ p_2\ p_3 \ldots p_t$ $\longrightarrow$ $\phi(m) = (p_1 - 1)\,(p_2 - 1)\,(p_3 - 1) \ldots\ldots$

Order of elements in the Ring of Integers modulo m: Z_m

The invertible elements in Z_m build a multiplicative group called Z^*_m with the following properties:

- The number of elements in Z^*_m is $\phi(m)$
- Z^*_m is a cyclic group if it contains an element with the order $\phi(m)$
- The order of any element in Z^*_m divides $\phi(m)$
- If the order of α is k then $Ord(\alpha^i) = k / gcd(i,k)$
  special case: If the order of α is k then the other elements with order k are (α^i) where $gcd(i,k) = 1$
- Number of elements with order k is $= \phi(k)$ if Z^*_m is a cyclic group

Summary: Euler and Carmichael Theorems

Euler's Theorem

For any unit **u** in Z_m where **gcd (m, u) = 1** (or for any element in Z^*_m) , the following holds:

$u^{\phi(m)} = 1$ (in Z_m)

Fermat 's Theorem (a special case of Euler's theorem):

For m=p, where p is prime => $u^{p-1} = 1$ in Z_p for any integer u

Carmicheal´s Theorem

The greatest order of an elements in Z^*_m is called Carmichael´s function $\lambda(m)$:
$\lambda(m)$ divides $\phi(m)$, **for any** $u \in Z^*_m$, $u^{\lambda(m)} = 1$ in Z^*_m

Carmicheal´s function $\lambda(m)$:

$\lambda(2) = 1$, $\lambda(2^2) = 2$, $\lambda(2^e) = 2^{e-2}$ for $e \geq 3$:

$\lambda(p^e) = \Phi(p^e) = (p - 1)p^{e-1}$ for p odd prim.

for $m = p_1^{e1}\ p_2^{e2}\ p_3^{e3} \ldots p_n^{en}$

$\lambda(m) = lcm\,[\,\lambda(p_1^{e1}), \lambda(p_2^{e2}), \ldots \lambda(p_n^{en})\,]$

$$\mathrm{lcm}(a,b) = \frac{a \cdot b}{\gcd(a,b)}.$$

Problem 2-1: Elements of Z_{33}

1. How many invertible element under multiplication do exist in Z_{33} (number of units in Z_{33})?
2. Which multiplicative orders are possible in Z^*_{33}?
3. Compute the order of the element 2, 5 and 7 in Z_{33}.
4. Compute 3 other elements having the same order as 2, 5, and 7.
5. Compute the order of the elements 10,32,23.
6. Compute the order of elements 4 and other elements having the same order.

Solution 2-1:

1. Number of invertible elements (units) is Euler function **$\phi(33) = \phi(3*11) = (3-1)(11-1) = 20$**
   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 } = Z^*, (gcd (33,u) = 1)
2. Possible multiplicative orders of units in Z_{33} are the divisors of $\lambda(33) = lcm[\phi(11), \phi(3)] = lcm(10,2) = 0*2/gcd(10,2) =$ **10**
   => Possible orders are the divisors of 10, which are **1, 2, 5, 10**
3. Order of 2: $2^1 = 2 \neq 1$, $2^2 = 4 \neq 1$, $2^5 = 32 = -1 \neq 1$ => **order of 2 is 10**
   Order of 5: $5^1 = 5 \neq 1$, $5^2 = 25 = -8 \neq 1$, $5^5 = -2*5 = -10 = 23 \neq 1$ => **order of 5 is 10**
   Order of 7: $7^1 = 7 \neq 1$, $7^2 = 49 = 16 \neq 1$, $7^5 = 13*16 = 10 \neq 1$ => **order of 7 is 10**
4. If order α = k, then ord (α^i) = k iff gcd(k,i) = 1. By selecting i = 1,3,7,9 we get gcd(10,i) = 1.
   => $2^1, 2^3, 2^7, 2^9$ **or 2 , 8 , 29 , 17 are 4 elements having order 10**
   => $5^1, 5^3, 5^7, 5^9$ **or 5, 26 , 14 , 20 are 4 elements having order 10**
   => $7^1, 7^3, 7^7, 7^9$ **or 7 , 13 , 28 , 19 are 4 elements having order 10**
5. Order of 10: $10^1 = 10 \neq 1$, $10^2 = 100 = 1$ => **order of 10 is 2**
   Order of 32: $32^1 = 32 = -1 \neq 1$, $32^2 = 1$ => **order of 32 is 2**
   Order of 23: $23^1 = 23 = -10 \neq 1$, $23^2 = (-10)^2 = 100 = 1$ => **order of 23 is 2**
6. Order of 4: $4^1 = 4 \neq 1$, $4^2 = 16 \neq 1$, $4^5 = 25*4 = 100 = 1$ => **order of 4 is 5**
   For gcd(5,i) = 1 => i = 1,2,3,4 => $4^1, 4^2, 4^3, 4^4$ or **4 , 16 , 31 , 25 are elements having order 5**

Notice: No. of elements having order 10 is not $\phi(10)$ as Z^*_{33} is not a cyclic group

Problem 2-2: Elements of Z_{17} = GF(17)

1. How many invertible element under multiplication do exist in GF(17) (number of units in GF(17))?
2. Which multiplicative orders are possible in GF(17)?
3. How many elements do exist from each possible order?
4. Compute the order of the element 2 in GF(17).
5. Compute all other elements having the same order as 2.

Solution 2-2:

1. Number of invertible elements is Euler function **$\phi(17) = (17-1) = 16$**
2. The possible multiplicative orders in GF(17) are the divisors of **$\phi(17)$** = 17 – 1 = **16**, namely **1, 2, 4, 8, 16**
3. 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 8 is **$\phi(8) = \phi(2^3) = 8\,(1-1/2) = 4$**
   Number of elements with order 16 is **$\phi(16) = \phi(2^4) = 16\,(1-1/2) = 8$**
4. Order of 2: $2^1 = 2 \neq 1$, $2^2 = 4 \neq 1$, $2^4 = 4^2 = 16 = -1 \neq 1$, $2^8 = (2^4)^2 = -1^2 = 1$ => **order of 2 is 8**
5. 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.
   => $2^1, 2^3, 2^5, 2^7$ **or 2 , 8 , 15 , 9 are the 4 elements having order 8**

Problem 2-3: Elements of GF(23)

1. How many invertible element under multiplication do exist GF(23) (number of units in GF(23))?
2. Which multiplicative orders are possible in GF(23)?
3. How many elements do exist from each possible order?
4. Compute the order of the element 2 in GF(23).
5. Compute all other elements having the same order as 2.
6. Compute the inverse of 2^{18} in GF(23) without using the gcd algorithm.

Solution 2-3:

1. Number of invertible elements is Euler function **$\phi(23) = (23-1) = 22$ elements**
2. The possible multiplicative orders in GF(23) are the divisors of 23 – 1 = 22, namely **1, 2, 11, 22**
3. 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 11 is **$\phi(11) = (11-1) = 10$**
   Number of elements with order 22 is **$\phi(22) = \phi(2*11) = (2-1)(11-1) = 10$**
4. Order of 2: $2^1 = 2 \neq 1$, $2^2 = 4 \neq 1$, $2^4 = 16 = -7$, $2^5 = -14 = 9$, $2^{10} = 81 = 12$, $2^{11} = 12*2 = 24 = 1$ => **order of 2 is 11**
5. If order α = k, then ord (α^i) = k iff gcd(k,i) = 1. By selecting i = 1,2,3,4,5,6,7,8,9,10 we get gcd(11,i) = 1.
   => $2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}$ **or 2,4,8,16,9,18,13,3,6,12 are the 10 elements having order 11**
6. The inverse of 2^{18} is 2^{-18} . The modulus in the exponent is **$\phi(23) = 23-1 = 22$**
   $2^{-18} = 2^{-18+22} = 2^4 = 16$. Check $2^{18} = (2^9)^2 = 6^2 = 13$ => $16*13 = 208 = 1$ in GF(23).

Homework: Elements of Z_{35}

1. How many invertible element under multiplication do exist Z_{35} (number of units in Z_{35})?
2. Which multiplicative orders are possible in Z^*_{35}?
3. Compute the order of all invertible elements in Z^*_{35}.
4. Find the cycle length for all non-invertible elements.

Homework: Elements of Z_{39}

1. How many invertible element under multiplication do exist Z_{39} (number of units in Z_{39})?
2. Which multiplicative orders are possible in Z^*_{39}?
3. Compute the order of all invertible elements in Z^*_{39}.
4. Find the cycle length for all non-invertible elements.

Homework: **Analyze the structure of GF(29), GF(83), $Z_{2^{16}}$**

Z_{2^n} **Is a widely used ring in modern cryptography**