Euler's Totient Function

Debdeep Mukhopadhyay

Associate Professor
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
INDIA -721302

Objectives

- **Euler's Totient Function**

Invertibility modulo m

- **Defn: An element a ε Z_m, is said to be invertible modulo m (or a unit in Z_m) if there exists an integer u (in Z_m), such that ua≡1 (mod m)**
- **Theorem: An element a ε Z_m is invertible iff gcd(a,m)=1.**

Reduced Residue System

- **A set of integers a1, a2, …, al is called a reduced residue system mod m if every integer a coprime to m is congruent to one and only one of the elements ai, *1≤ i ≤ l.***
- **Elements of a reduced residue system are all coprime to m, and are not congruent to each other, mod m.**

Euler's Totient function

- Suppose a≥1 and m≥2 are integers. If gcd(a,m)=1, then we say that a and m are relatively prime.
- The number of integers in Z_m (m>1), that are relatively prime to m is denoted by Φ(m), called Euler's Totient function or phi function.
- Φ(1)=1

Example

- m=26 => Φ(26)=12
- If p is prime, Φ(p)=p-1
- If n=1,2,…,24 the values of Φ(n) are:
  - 1,1,2,2,4,2,6,4,6,4,10,4,12,6,8,8,16,6,18,8, 12,10,22,8
  - Thus we see that the function is very irregular.

Properties of Φ

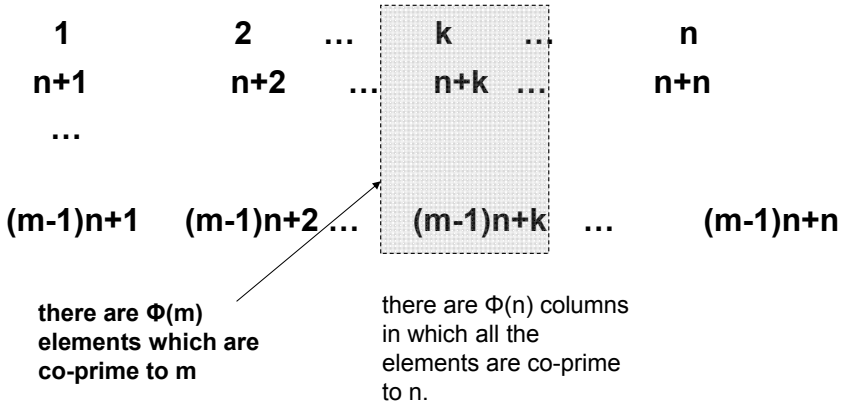
- **If m and n are relatively prime numbers,**
  - **Φ(mn)= Φ(m) Φ(n)**
- **Φ(77)= Φ(7 x 11)=6 x 10 = 60**
- **Φ(1896)= Φ(3 x 8 x 79)=2 x 4 x 78 =624**
- **This result can be extended to more than two arguments comprising of pairwise coprime integers.**

Results

- **If there are m terms of an arithmetic progression (AP) and has common difference prime to m, then the remainders form Z_m.**
- **An integer a is relatively prime to m, iff its remainder is relatively prime to m**
- **If there are m terms of an AP and has common difference prime to m, then there are Φ(m) elements in the AP which are relatively prime to m.**

An Important Result

- **If m and n are relatively prime, Φ(mn)=Φ(m)Φ(n)**



contd.

- **Thus, there are Φ(n) columns with Φ(m) elements in each which are co-prime to both m and n.**
- **Thus there are Φ(m) Φ(n) elements which are co-prime to mn.**
  - **This proves the result…**

Further Result

- $\Phi(p^a)=p^a-p^{a-1}$
  - Evident for a=1
  - For a>1, out of the elements 1, 2, …, p^a the elements p, p^2, $p^{a-1}p$ are not co-prime to p^a.

  Rest are co-prime.

  Thus $\Phi(p^a)=p^a-p^{a-1}$

  $=p^a(1-1/p)$

contd.

- $n=p_1^{a1}p_2^{a2}\ldots p_k^{ak}$
- Thus, $\Phi(n)= \Phi(p_1^{a1})\ \Phi(p_2^{a2})\ \ldots\ \Phi(p_k^{ak})$

  $=n(1-1/p_1)(1-1/p_2)\ldots(1-1/p_k)$

Thus, if m=60=4x3x5

$\Phi(60)=60(1-1/2)(1-1/3)(1-1/5)=16$

Fermat's Little Theorem

- If gcd(a,m)=1, then $a^{\Phi(m)} \equiv 1 \pmod{m}$.
- Proof: $R=\{r_1,\ldots,r_{\Phi(m)}\}$ is a reduced residue system (mod m).
- If gcd(a,m)=1, we see that $\{ar_1,\ldots,ar_{\Phi(m)}\}$ is also a reduced system (mod m).
- It is a permutation of the set R.
- Thus, the product of the elements in both the sets are the same.

  Hence, $a^{\Phi(m)}\, r_1,\ldots,r_{\Phi(m)} \equiv r_1,\ldots,r_{\Phi(m)} \pmod{m}$

  $\Rightarrow a^{\Phi(m)} \equiv 1 \pmod{m}$

  Note we can cancel the residues as they are co-prime with m and hence have multiplicative inverse.

Example

- Find the remainder when 72^{1001} is divided by 31.
- Since, $72 \equiv 10 \pmod{31}$. Hence, $72^{1001} \equiv 10^{1001} \pmod{31}$.
- Now from Fermat's Theorem, $10^{30} \equiv 1 \pmod{31}$ [note 31 is prime]
- Raising both sides to the power 33,

  $10^{990} \equiv 1 \pmod{31}$

Thus,

$10^{1001}=10^{990}10^{8}10^{2}10=1(10^{2})^{4}10^{2}10=1(7)^{4}7.10=49^{2}.7.10=(-13)^{2}.7.10=(14.7).10=98.10=5.10=19 \pmod{31}$.

Cyclic Group

- **If p is prime, then Z_p^* is a group of order p-1 and any element in Z_p^* has an order which divides (p-1).**
- **In fact, if p is prime, then there exists at least one element in Z_p^* which has order equal to p-1.**
  - **this is called cyclic group…**

Primitive Element

- **If p is prime, then Z_p^* is a cyclic group.**
- **Any element α having order p-1 mod p is called a primitive element. Thus α is a primitive element iff:**

$$\{\alpha^i : 0 \leq i \leq p-2\} = \mathbb{Z}_p^*$$

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

- **n=19, There are 6 primitive elements.**
- **Note the order of each element in Z_{19}^*.**
- **Is there a relation?**

Order of any element

- **Any element β in Z_p^* (where p is prime) can be written uniquely in the form $\beta=\alpha^i$, where α is a primitive element and $0 \le i \le p-2$.**
- **The order of β is:**

$$\frac{p-1}{\gcd(p-1,i)}$$

- **β is itself primitive iff gcd(p-1,i)=1. Hence, what is the number of primitive elements modulo p?**

Example

- **p=13**
- **Thus $\Phi(13-1)= \Phi(12)= \Phi(3x2^2)=12(1-1/3)(1-1/2)=12x(2/3)x(1/2)=4$.**
- **Question: Is 2 a primitive element of Z_{13}^*?**
  - **generate all the (p-1) powers of 2.**
  - **lengthy process if p is large.**

Theorem

THEOREM 5.8 *Suppose that $p > 2$ is prime and $\alpha \in \mathbb{Z}_p^*$. Then α is a primitive element modulo p if and only if $\alpha^{(p-1)/q} \not\equiv 1 \pmod{p}$ for all primes q such that $q \mid (p-1)$.*