Introduction to Number Theory

Contd…

Euler's Phi-Function Ø(n)

- Euler's Phi-Function of positive integer n, is denoted by Ø(n), which is equal to the number of positive integers less than n and relatively prime to n.

Euler’s Phi-Function

1. $\phi(1) = 0$.
2. $\phi(p) = p - 1$ if p is a prime.
3. $\phi(m \times n) = \phi(m) \times \phi(n)$ if m and n are relatively prime.
4. $\phi(p^e) = p^e - p^{e-1}$ if p is a prime.

Contd.

- Note: We can also combine the rules to find Ø(n)
- What is the value of Ø (13)?
- We can use the third rule: Ø (10) = Ø (2) × Ø (5) = 1 × 4 = 4, because 2 and 5 are primes.
- Ø(49).....?

Sieve of Eratosthenes

Greek Mathematician

Goal: Given a number n, print all primes smaller than or equal to n.

Suppose we want to find all primes less than 100.

Compute square root of 100 = 10

We need to see if any number less than 100 is divisible by 2,3,3,5 and 7

We create a list of all numbers from 2 to 100

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Contd.

Sieve process is as follows:

1. Cross out all numbers divisible by 2 (except 2 itself)
2. Cross out all numbers divisible by 3 (except 3 itself)
3. Cross out all numbers divisible by 5 (except 5 itself)
4. Cross out all numbers divisible by 7 (except 7 itself)
5. **The numbers left over are primes.**

Congruence Relation

- *For a positive integer n, two integers 'a' & 'b' are said to be congruent modulo 'n', written:*

$$a \equiv b \bmod n$$

If they leaves the same remainder when divided by n.

- Note: The set consisting of the integers congruent to ‘a’ modulo ‘n’, is called the congruence class or residue class of ‘a’ modulo n.
- Denotes by Z_n
- Congurence operator maps a member of Z to a member of Z_n

Properties of Congruences

- $\forall\ a, b, a_1, b_1, c \in Z$ following are true
- (reflexivity) $a \equiv a (\text{mod } n)$;
- (symmetry) if $a \equiv b (\text{mod } n)$, then $b \equiv a (\text{mod } n)$;
- (transitivity) if $a \equiv b (\text{mod } n)$ and $b \equiv c (\text{mod } n)$ then $a \equiv c (\text{mod } n)$;

Modular exponentiation

- Find $7^{29} \pmod{17}$
- Sol: $7^1 \pmod{17} = 7$
  $7^2 \pmod{17} \equiv 49 \pmod{17} = 15$
  $7^4 \pmod{17} \equiv 7^2 * 7^2 \pmod{17} \equiv 15 * 15 \pmod{17} = 4$
  $7^8 \pmod{17} \equiv 7^4 * 7^4 \pmod{17} \equiv 4*4 \pmod{17} = 16$
  $7^{16} \pmod{17} \equiv 7^8 * 7^8 \pmod{17} \equiv 16*16 \pmod{17} = 1$
- Then, $7^{29} \pmod{17} \equiv 7^{16} * 7^8 * 7^4 * 7^1 \pmod{17} \equiv 1 * 16 * 4 * 7 \pmod{17} \equiv 448 \pmod{17} = 6.$

Set of residues

Define the set Z_n as the set of nonnegative integers less than n:

$$Z_n = \{0, 1, \ldots, (n-1)\}$$

This set is referred to as the set of **residues**, or **residue classes** (mod *n*). That is, each integer in Z_n represents a residue class.

Additive inverse modulo n

- Definition : An integer b is an additive inverse to a modulo n,

  if $a+b \equiv 0 \pmod{n}$.

  In Z_n every integer will have a unique additive inverse modulo n.

Addition modulo 4 : addition in Z_4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

- Additive inverse of 1 is 3
- Additive inverse of 2 is 2
- Additive inverse of 3 is 1
- Each element has a additive inverse

Multiplicative inverse modulo n

- Definition : An integer x is a (multiplicative) inverse to a modulo n,

  $$\text{if } a.x \equiv 1 \pmod{n}$$

  and we denote x by a^{-1}.
- Example: Find the multiplicative inverse of 14 modulo 9
- Sol: Find an integer x in Z_9 such that

  $$14.x \equiv 1 \pmod{9}$$

  since $14.2 = 28 \equiv 1 \pmod{9}$, 2 is the multiplicative inverse of 14 modulo 9.

Criterion for Invertibility mod n:

- There is no multiplicative inverse to 2 (mod 4).
- Suppose **a** and **n** are integers and n> 1. Then **a** has an inverse modulo **n** if and only if gcd(a, n) = 1. Moreover, if gcd(a, n) = 1, then a has a unique inverse, x in Z_n.

Multiplication in Z_4

Multiplication modulo 4

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

- 2 has no inverse in Z_4
- (2 has no inverse modulo 4)
- Inverse of 1 is 1
- Inverse of 3 is 3

Multiplication in Z_5

Multiplication modulo 5

- Every non zero element of Z_5 has inverse in $Z_{5,}$
- Inverse of 2 is 3, inverse of 3 is 2, inverse of 4 is 4.

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

A Multiplication Table in Z_n: Summary

- The numbers that have inverses in Z_n are **relatively prime** to n

  That is: gcd(x, n) = 1

- If n is a prime number than every non zero element of Z_n will have a unique inverse in Z_n.
- Few More Sets......... Z_P, Z_n^*, Z_P^*