Discrete Structures

Day 3

Euler's Phi function $\emptyset(n)$/Euler's totient function

- Euler's Phi function finds the number of integers that are both smaller than 'n' and relatively prime to 'n'.

Some rules to find $\emptyset(n)$

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

If *n* can be factored as $n = p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_k^{e_k}$,combine third and forth rule to find

$$\emptyset(n) =(p_1^{e_1} - p_1^{e_1-1}) \times (p_2^{e_2} - p_2^{e_2-1}) \times \cdots \times (p_k^{e_k} - p_k^{e_k-1})$$

Q. What is the value of

i. $\emptyset(13) = (13 - 1) = 12$

ii. $\emptyset(10) = \emptyset(2) \times \emptyset(5) = 1 \times 4 = 4$

iii. $\emptyset(240) = ?$

Fermat's Little Theorem

First theorem: If p is a prime and a is an integer such that p does not divide a, then $a^{p-1} \equiv 1 \ mod \ p$

Second theorem: If p is a prime and a is an integer, then $a^{p} \equiv a \ mod \ p$

Q. Find

i. $6^{10} \ mod \ 11$

ii. $3^{12} \ mod \ 11 = (3 \times 3^{11}) \ mod \ 11 = (3 \ mod \ 11 \times 3^{11} \ mod \ 11) \ mod \ 11$

$= (3 \times 3) \ mod \ 11 = 9$

iii. $7^{28} \ mod \ 13 = ?$

Some multiplicative inverse can be solved using Fermat's Little Theorem if the modulus is prime. If p is the prime and a is an integer such that $p \nmid a$ then $a^{-1} mod\ p = a^{p-2} mod\ p$

Derived from Fermat's first theorem

$$a^{p-1} \equiv 1\ mod\ p$$

iff

$$a^{p-1} mod\ p = 1\ mod\ p$$

Multiplying both sides by a^{-1}, $a^{p-2} mod\ p = a^{-1} mod\ p$

Q. Find $8^{-1} mod$ 17 without using extended Euclidean algorithm.

Euler's theorem

- First version: If a and n are coprime, then $a^{\phi(n)} \equiv 1 \; mod \; n$

Second version: If $n = p \times q, a < n,$ and k an integer, then

$$a^{k \times \phi(n)+1} \equiv a \; mod \; n$$

Q. Find

i. $6^{24} mod \; 35$

$$= 6^{\phi(35)} mod \; 35 = 1$$

ii. $20^{62} mod \; 77$

- Some multiplicative inverse can be solved using Euler's Theorem. If *n* and *a* are coprime, then $a^{-1} mod\ n = a^{\phi(n)-1} mod\ p$

Q. Find $7^{-1} mod\ 15$ without using extended Euclidean algorithm.

Applications of Congruence's

- **Hashing Functions**

  One of the most commonly used hashing functions

  $$h(k) = k \textbf{ mod } m$$

- A hashing function h assigns memory location $h(k)$ to the record that has k as its key.
- *Eg:* Assigning a memory locations in a central computer so that customer records can be retrieved quickly. Customer records are often identified using the Social Security number of the customer as the key (k) where m is the number of available memory locations.

- Hashing functions should be easily evaluated so that files can be quickly located.
- Q. Find the memory locations assigned by the hashing function $h(k) = k \textbf{ mod } 111$ to the records of customers with Social Security numbers 064212848 and 037149212.

  $h(064212848) = 064212848 \textbf{ mod } 111 = 14.$

  $h(037149212) = 037149212 \textbf{ mod } 111 = 65,$

- **Pseudorandom Numbers:** Numbers generated by systematic methods that are not truly random.

- The most commonly used procedure for generating pseudorandom numbers is the **linear congruential method**. We choose four integers: the **modulus** m, **multiplier** a, **increment** c, and **seed** $x0$, with $2 \le a < m$, $0 \le c < m$, and $0 \le x0 < m$.
  - recursively defined function $x_{n+1} = (ax_n + c)\ mod\ m$
- Eg: Find the sequence of pseudorandom numbers generated by the linear congruential method with modulus $m = 9$, multiplier $a = 7$, increment $c = 4$, and seed $x0 = 3$.

$$
\begin{aligned}
x1 &= 7x0 + 4 \textbf{ mod } 9 = 7 \cdot 3 + 4 \textbf{ mod } 9 = 25 \textbf{ mod } 9 = 7,\\
x2 &= 7x1 + 4 \textbf{ mod } 9 = 7 \cdot 7 + 4 \textbf{ mod } 9 = 53 \textbf{ mod } 9 = 8,\\
x3 &= 7x2 + 4 \textbf{ mod } 9 = 7 \cdot 8 + 4 \textbf{ mod } 9 = 60 \textbf{ mod } 9 = 6,\\
x4 &= 7x3 + 4 \textbf{ mod } 9 = 7 \cdot 6 + 4 \textbf{ mod } 9 = 46 \textbf{ mod } 9 = 1,\\
x5 &= 7x4 + 4 \textbf{ mod } 9 = 7 \cdot 1 + 4 \textbf{ mod } 9 = 11 \textbf{ mod } 9 = 2,\\
x6 &= 7x5 + 4 \textbf{ mod } 9 = 7 \cdot 2 + 4 \textbf{ mod } 9 = 18 \textbf{ mod } 9 = 0,\\
x7 &= 7x6 + 4 \textbf{ mod } 9 = 7 \cdot 0 + 4 \textbf{ mod } 9 = 4 \textbf{ mod } 9 = 4,\\
x8 &= 7x7 + 4 \textbf{ mod } 9 = 7 \cdot 4 + 4 \textbf{ mod } 9 = 32 \textbf{ mod } 9 = 5,\\
x9 &= 7x8 + 4 \textbf{ mod } 9 = 7 \cdot 5 + 4 \textbf{ mod } 9 = 39 \textbf{ mod } 9 = 3.
\end{aligned}
$$

The sequence :3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, . . .

Check Digits

- Congruences are used to check for errors in digit strings. A common technique for detecting errors in such strings is to add an extra digit at the end of the string. This final digit, or check digit, is calculated using a particular function. Then, to determine whether a digit string is correct, a check is made to see whether this final digit has the correct value.
- Eg: **ISBNs** All books are identified by an **International Standard Book Number (ISBN-10)**, a 10-digit code $x1x2 \dots x10$, assigned by the publisher.
- The check digit is calculated as:

$x_{10} \equiv \sum_{i=1}^{9} ix_i mod\ 11$ (either a digit or the letter X (used to represent 10)).

$$\sum_{i=1}^{10} ix_i mod\ 11 \equiv 0\ mod\ 11$$

Q. Answer these questions about ISBN-10s:

i. The first nine digits of the ISBN-10 of the sixth edition of this book are 007288008. What is the check digit?

$$x_{10} \equiv (1 \times 0 + 2 \times 0 + 3 \times 7 + 4 \times 2 + 5 \times 8 + 6 \times 8 + 7 \times 0 + 8 \times 0 + 9 \times 8) mod\ 11 \equiv 182\ mod\ 11 \equiv 2$$

ii. Is 084930149X a valid ISBN-10?

Cryptography

- Transforming information so that it cannot be easily recovered without special knowledge.

- **Classical Cryptography**
- One of the earliest known uses of cryptography was by Julius Caesar. He made messages secret by shifting each letter three letters forward in the alphabet
- $f(p) = (p + 3) \ \mathbf{mod}\ 26.$
- Encryption: The process of making a message secret.

Q. What is the secret message produced from the message "PARK" using the Caesar cipher? (Assume A, B, C, . . . , Z = 0, 1, 2, . . ., Z)

- PARK integer representation: 15, 0, 17, 10
- $f(p) = (p + 3)$ **mod** 26

  18, 3, 20, 13

  S D U N

Q. What is the plain message if the cipher text is "WKH" encrypted using Caesar cipher?

RSA
(Rivest Shamir Adleman) cryptosystem

RSA is one of the first public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and distinct from the decryption key which is kept secret. Invented by Rivest, Shamir and Adleman.

Key generation, encryption and decryption algorithm

Key Generation

Select p, q	p and q both prime
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \bmod \phi(n)$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext	$M < n$
Ciphertext	$C = M^e \pmod{n}$

Decryption

Ciphertext	C
Plaintext	$M = C^d \pmod{n}$

- Example
  - Bob chooses 7 and 11 as p and q and calculates n = 7*11=77.
  - The value of $\varphi(n) = (7-1)(11-1) = 60.$
  - Bob choses e=13 and computes d :
  - $d \equiv e^{-1} \mathrm{mod} \varphi(n)$

    i.e. $d \equiv 13^{-1} \mathrm{mod}\ 60$ (apply Extended Euclidean algorithm to find the inverse.

    On computation you will get d=37.

    Bob announces ‘e’ and ‘n’ as public and keeps ‘d’ as secret key.

- Imagine Alice wants to send the plaintext (M) 5 to Bob. She use the public key of Bob to generate the cipher text 'C' given by the formula $C = M^e mod\, n$.

So, $C = 5^{13} mod\ 77$

Cipher text $C = 26$.

- Bob on receiving the ciphertext $C = 26$, uses his secret/private key to decipher.
- Plaintext $\mathrm{M} = C^d mod\ n$

$M = 26^{37} mod\ 77$

M = 5 (which is the plaintext sent by Alice).

Let p=23, q = 31, Bob Choses e=83. Compute d? If Alice wants to sent the text “CSE”, the ASCII code is (67, 83, 69). Find the cipher text for each ASCII code. Convert back the cipher text to plaintext using the private key ‘d’