Week 2

Lecture 2
Properties of Numbers II
Udaya Parampalli

School of Computing and Information Systems
University of Melbourne

Week 2

Lecture 1

Part -1 Extended GCD Algorithm and Related Computations

Part -2 Symmetric key Cryptography

Lecture 2
Properties of Numbers

Workshop 2: Workshops start from this week

Quizz 2

2.1 More on Inverse Modulo n

Modular Arithmetic

Let a and b be integers and let n be a positive integer. We say "a" is congruent to "b", modulo n and write

$$a \equiv b \ (mod \quad n),$$

if a and b differ by a multiple of n; i.e ; if n is a factor of $|b - a|$. Every integer is congruent mod n to exactly one of the integers in the set

$$Z_n = \{0, 1, 2, \cdots, n-1\}.$$

We can define the following operations:

$$x \oplus_n y = (x + y) \ mod \ \ n.$$

$$x \otimes_n y = (xy) \ mod \ \ n$$

When the context is clear we use the above special addition and multiplication symbols interchangeably with their counterpart regular symbols.

Modular Multiplicative Inverse

Definition

Let $x \in Z_n$, if there is an integer y such that

$$x \otimes_n y = 1,$$

then we say y is the multiplicative inverse of x. It is denoted by $y = x^{-1}$ usually.

Example: let $n = 5$, 2 is inverse of 3 in Z_5. Or in other words 2 is inverse of 3 modulo 5.

Determining multiplicative inverse

Fact

For any integers a and b, there exist integers x and y such that

$$gcd[a, b] := ax + by.$$

You can determine x and y by modifying Euclid‘s algorithm for $gcd(a, b)$. Thus we can say that we can find inverse of a modulo b provided $gcd(a, b) = 1$.

2.2 Euler's Phi Function

Euler Phi function

Definition

Two numbers a and b are relatively prime if $gcd(a, b)$ *is* 1.

Definition

Euler phi function(or Euler totient function): For $n \geq 1$*, let* $\phi(n)$ *denote the number of integers less than n but are relatively prime to n.*

Definition

Reduced set of residues mod n: For $n \geq 1$*, the reduced set of residues,* $R(n)$ *is defined as set of residues modulo n which are relatively prime to n.*

Example: $\phi(6) = 2$: Observe, $gcd(1, 6) = 1, gcd(2, 6) = 2, gcd(3, 6) = 3, gcd(4, 6) = 2, gcd(5, 6) = 1$. Then $R(6) = \{1, 5\}$. Hence $\phi(6) = 2$.

Some Relations

Fact

$\phi(p) = p - 1$, *for any prime p.*

This is easy and follows from definition of a prime number.

Fact

$$\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1),$$

for any prime p and any integer $a \geq 1$.

Consider numbers from 0 to $p^a - 1$, then only numbers which have some common divisor with p^a are those numbers which are multiple of p. There are exactly p^{a-1} such numbers including the number 0. All other numbers are relatively prime to p^a. Hence, $\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$ as needed.
Example: $\phi(8) = 4$, the numbers which are multiple of 2 are $\{2, 4, 6, 8\}$ and hence the relatively prime numbers are all odd numbers up to 7, i.e $R(8) = \{1, 3, 5, 7\}$.

Some Relations, cont.

Fact

$\phi(pq) = (p-1)(q-1)$, *for any pair of primes p and q.*

Proving this result is trickier than before but still not difficult to visualize. Again consider numbers from 1 to pq. Like before, we can exclude all those numbers which are multiple of p and q to form $R(pq)$. Then can we say the folowing?

$$|R(pq)| = pq - ((pq)/q) - ((pq)/p) = (pq - p - q)$$

In the above counting, we have excluded multiple of pq twice, once while excluding the multiples of p and again while excluding the multiples of q. So we need to make the following change

$$\phi(pq) = |R(pq)| = pq - p - q + 1 = (p-1)(q-1).$$

Example: $\phi(15) = 8$, the relatively prime numbers are $1, 2, 4, 7, 8, 11, 13, 14$.

Euler Phi function is multiplicative

Fact

If a and b are relatively prime numbers ($gcd(a, b) = 1$), then,

$$\phi(ab) = \phi(a)\phi(b).$$

This is not directly obvious with whatever we have studied so far. But take this as a fact. You can prove this using some elementary number theory results.
Using the above fact, we can derive a general result about eulers ϕ function. We know that any number has a unique factorization:

$$n = \Pi_{i=1}^{\tau} p_i^{a_i} = p_1^{a_1} \ p_2^{a_2} \cdots p_\tau^{a_\tau} \ ,$$

where τ is a positive number, p_i are primes and $a_i \geq 1$ and Π is the symbol for product. Find $\phi(n)$ for this case. Example: What is $\phi(200) = \phi(2^3 \ 5^2)$?.

Euler Phi function for general n

Using the multiplicative property of ϕ, we can simplify $\phi(n)$ as follows:

$$\phi(n) = \phi(\Pi_{i=1}^{\tau} p_i^{a_i}) = \phi(p_1^{a_1}\ p_2^{a_2} \cdots p_\tau^{a_\tau}),$$

From the fact on $\phi(p^a)$ given before we can write,

$$\phi(n) = \Pi_{i=1}^{\tau} p_i^{a_i - 1}(p_i - 1))).$$

Example: What is $\phi(200) = \phi(2^3\ 5^2) = \phi(2^3)\phi(5^2) = 80.$

2.3 How can you use Euler's Phi to compute inverses?

We have seen how Extended GCD Algorithm to compute $inverse(a) \,/ \bmod n$ before.
We will prove the following result later, but let us state it now. let $\mathbf{Z}_n^\star$ be set of numbers from 1 to $n-1$ but are relatively prime.

Theorem

If $a \in \mathbf{Z}_n^\star$, then $a^{\phi(n)} = 1 \pmod n$.

Now, how can you use the above theorem for computing inverse of $a \mod n$?

$inverse(a) \mod n$

Given a a number less than n but relatively prime to n

$Function(a, n)$
$inva := a^{\phi(n)-1} \pmod{n}.$
$Return(inva);$
$end\ \ function;$

Week 1

Lecture 1

Part -1 Extended GCD Algorithm and Related Computations

Part -2 Symmetric key Cryptography

Lecture 2
Properties of Numbers

Workshop 2: Workshops start from this week

Quizz 2