Properties of Numbers, continued

Udaya Parampalli

Department of Computing and Information Systems
University of Melbourne

July, 2017

THE UNIVERSITY OF MELBOURNE

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 $gcd(a, b) = 1$.

Euclid's algorithm, takes two inputs $a[1], a[2]$ and returns $gcd(a[1], a[2])$ and $x[1], x[2]$ such that

$$gcd[a[1], a[2]] := x[1]a[1] + x[2]a[2].$$

Plsease read the slides on recursion to implement the algorithm.

Computing inverse mod n

If $gcd(n, a)$ is 1 then we can use extended Euclid's algorithm on a and n and get two integers x and y such that

$$xn + ya = 1.$$

Taking mod n on both sides of the above equation we get

$$ya = 1 \bmod n.$$

Clearly y is the inverse of a mod n. Note that the inverse is unique. Also it is clear that if $gcd(n, a) > 1$, then inverse does not exist.

Computing inverse mod n

If $gcd(a, n)$ is 1 then we can use extended Euclid's algorithm on a and n and get two integers x and y such that

$$xa + yn = 1.$$

Taking mod n on both sides of the above equation we get

$$xa = 1 \bmod n.$$

Clearly y is the inverse of a mod n.

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 $\phi(6) = 2$.

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 $R(8) = \{1, 3, 5, 7\}$.

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 0 to $pq-1$. Like before, we can exclude all those numbers which are multiple of p and q to form $R(pq)$. Then can we say that

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

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 have

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

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 $\phi(200) = \phi(2^3\ 5^2) = \phi(2^3)\phi(5^2) = 80.$

Functions

Definition: A function is defined by a triplet $< X, Y, f >$, where X: a set called domain; Y: a set called range or codomain and f: a rule which assigns to each element in X precisely one element in Y.

It is denoted by $f : X \to Y$

Example: Let $X = Y = \mathbf{Z}_5$, Then $f : X \to Y$ given by $f(x) = 2 * x$ is a function.

Definitions

Image : If $x \in X$, the image of x in Y is an element $y \in Y$ such that $y = f(x)$.
Pre-image : If $y \in Y$, then a Pre-image of y in X is an element $x \in X$ such that $f(x) = y$.
Image of a function f **(**$Im(f)$: A set of all elements in Y which have at least one Pre-image.

$$Im(f) = \bigcup_{x \in X} \{f(x)\} \tag{1}$$

One-to-one (injective) Function

A function is one-to-one (injective) if each element in the codomain Y is the image of **at most** one element in the domian X. In other words, each element in x in X is related to different y in X, never two different elements in X map to a same element in Y. We can say that $|X| \leq |Y|$. An alternate definition would be, a $f : X \to Y$ is one-to-one (injective), provided

$$f(x_1) = f(x_2) \text{ implies } x_1 = x_2.$$

Examples: Let $X = Y = \mathbf{Z}_4$, Then $f : X \to Y$ given by $f(x) = 3 * x$ is a one-to-one function. However $f(x) = x^2$ is a not a one-to-one function.

Onto (surjective) Function

A function is Onto (surjective) if each element in the codomain Y is the image of **at least** one element in the domian X.
A function $f : X \to Y$ is onto if $Im(f) = Y$
We can say that, if f is onto then $|Y| \leq |X|$.
Example: Let $X = Y = \mathbf{Z}_5$, Then $f : X \to Y$ given by $f(x) = x^2$ is a onto function.
Bijection: A function which is both one-to-one and onto.
In this case, we have $|X| \leq |Y|$ and $|Y| \leq |X|$. This implies $|X| = |Y|$.
If $f : X \to Y$ is one-to-one then $f : X \to Im(f)$ is a bijection.
If $f : X \to Y$ is onto and X and Y are finite sets of the same size then f is a bijection.

Bijection

Let m and n are relatively prime number, $X = \mathbf{Z}_{mn}$, $Y = \mathbf{Z}_m \times \mathbf{Z}_n$. Then the mapping

$$f : X \to Y, f(x) = ((x \ mod \ m), x \ mod \ n),$$

is a bijection.

Example: $X := \mathbf{Z}_6$, $Y = \mathbf{Z}_2 \times \mathbf{Z}_3$. The function f given below is a bijection:

$X = \mathbf{Z}_6$	$\rightarrow$	$\mathbf{Z}_2 \times \mathbf{Z}_3$
0	$\rightarrow$	$(0, 0)$
1	$\rightarrow$	$(1, 1)$
2	$\rightarrow$	$(0, 2)$
3	$\rightarrow$	$(1, 0)$
4	$\rightarrow$	$(0, 1)$
5	$\rightarrow$	$(1, 2)$

Table: $f : \mathbf{Z}_6 \rightarrow \mathbf{Z}_2 \times \mathbf{Z}_3$

Chinese Remainder Theorem (CRT)

Let n_1, n_2 be pair-wise relatively prime integers, he system of simultaneous congruences

$$\begin{aligned} x &\equiv a_1 \; (mod \;\; n_1), \\ x &\equiv a_2 \; (mod \;\; n_2), \end{aligned}$$

has a unique solution modulo $n = n_1 \;\, n_2$.

Note that the mapping $f : \mathbf{Z}_{n_1\ n_2} \to \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2}$ given by $f(x)\ \to\ x\ mod\ n_1,\ x\ mod\ n_2$ is a bijection.
The proof has two points. First show that the function is one-to-one. If there exists two elements x and y such that

$$x\ mod\ n_1 = y\ mod\ n_1,$$

and

$$x\ mod\ n_2 = y\ mod\ n_2,$$

then $x - y$ is divisible by both n_1 and n_2. Since n_1 and n_2 are relatively prime, $x - y$ is divisible by $n_1\ n_2 = n$. Hence x and y are identical equal modulo n. This proves that the function is one-to-one. In the next slide, we give an explicit construction for the inverse function which proves that the map is onto. Hence the f is bijection.

In fact, Chinese Remainder theorem gives a construction method to obtain the inverse function. Let

$$N_1 = n/n_1 = n_2, N_2 = n/n_2 = n_1.$$

Choose

$$M_1 \;=\; (N_1)^{-1} \; (mod \;\; n_1)$$

and

$$M_2 \;=\; (N_2)^{-1} \; (mod \;\; n_2)$$

.

Then the solution to the simultaneous congruences is given by

$$x = a_1 \; (N_1 \;\; M_1) \; + a_2 \; (N_2 \;\; M_2) \;\; (mod \;\; n).$$

You can immediately verify that x determined as above satisfies the congruences (This is because $N_1 \;\; mod \;\; n_2 = 0$ and $N_2 \;\; mod \;\; n_1 = 0$)

Chinese Remainder Theorem (CRT)

If $n_1, n_2, \ldots, n_k$ are pair-wise relatively prime integers, k being a positive integer, the system of simultaneous congruences

$$\begin{aligned} x &\equiv a_1 \ (mod \ n_1), \\ x &\equiv a_2 \ (mod \ n_2), \\ x &\equiv a_3 \ (mod \ n_3), \\ &\ldots \\ x &\equiv a_k \ (mod \ n_k), \end{aligned}$$

has a unique solution modulo $n = n_1 \ n_2 \ \ldots \ n_k$.

Let

$$N_i = n/n_i$$

for $i = 1, 2, \ldots, k$.
Choose

$$M_i \ = \ (N_i)^{-1} \ (mod \ \ n_i),$$

for $i = 1, 2, \ldots, k$.
Then the solution is given by

$$x = \sum_{i=1}^{k} \ a_i \ N_i \ M_i \ \ (mod \ \ n).$$