Fermat and Euler theorems

Udaya Parampalli

Department of Computing and Information Systems
University of Melbourne

July, 2017

THE UNIVERSITY OF
MELBOURNE

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 $a \geq 1$.

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.*

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

where τ is a positive number, p_i are primes and $a_i \geq 1$ and Π is the symbol for product.

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

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

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

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:

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

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

Chinese Remainder Theorem (CRT)

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

$$x \equiv a_1 \ (mod \ n_1),$$

$$x \equiv a_2 \ (mod \ n_2),$$

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

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

Euler's Theorem

Theorem

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

Proof: Let $R(n) = \{r_1, r_1, \ldots, r_{\phi(n)}\}$,, be reduced set of residues modulo n. Now consider the set $a\ R(n) = \{a\ r_1, a\ r_1, \ldots, a\ r_{\phi(n)}\}$. Since a is relatively prime to n, the set $aR(n)$ is identically equal to $R(n)$. Note that the process of multiplying a only rearranges the residues in $R(n)$. Hence we can multiply all the elements in $R(n)$ and equate with the multiplication of all the elements of $a\ R(n)$. Hence we can write:

$$r_1 \times r_2 \cdots \times r_{\phi(n)} = (ar_1) \times (ar_2) \cdots \times (ar_{\phi(n)}).$$

Note that r_is are relatively prime to n and hence we can cancel r_i in the above equation by multiplying r_i^{-1} to both the side of the equation. Then the above equation simplifies to

$$1 = a^{\phi(n)}.\ \text{Hence the result.}$$

Fermat's Theorem

Theorem

Let p be a prime number, then if $gcd(a, p) = 1$, then

$$a^{p-1} = 1 \ (mod \ p).$$

This is the particular case of Euler's Theorem when n is prime.

Fermat's Little Theorem

Theorem

Let p be a prime number,

$$a^p = a \ (mod \ p), \ \ for \ any \ integer \ a.$$

When a is relatively prime, the theorem follows from the Fermatss theorem. When a is multiple of p, the result is trivially true.

RSA:Key Generation by entities

Before starting any transactions, Alice(A) and Bob (B) will set up the following key initializations.
Alice will do the following:

1. Generate two large and distinct primes p_A and q_A of almost equal size.
2. Compute $n_A = p_A q_A$ and $\phi_A = (p_A - 1)(q_A - 1)$.
3. Select a random integer e_A, such that $GCD[e_A, \phi_A] = 1$.
4. Compute the integer d_A such that
$$e_A d_A \equiv 1 \ (mod \ \phi_A).$$
(Use Extended Euclidean Algorithm).
5. **Alice's Public key is** (n_A, e_A)**.**
Alice's Private key is d_A.

Similarly, Bob will also initialize the key parameters. Let
Bob's Public key be (n_B, e_B) and
Bob's Private key be d_B,

RSA Public encryption

Here we assume that Bob wants to send a message to Alice.
Encryption at B

1. Get A's Public Key (n_A, e_A).
2. Choose a message M as an integer in the interval $[0, n_A - 1]$.
3. Compute $c = M^{e_A}\ (mod\ n_A)$.
4. Send the cipher text c to A.

Decryption at A

1. To recover m compute $M = c^{d_A}\ mod\ n_A$ using the secret d_A.

Proof of RSA Decryption

Since $e_A d_A \equiv 1 \ (mod \ \phi_A)$, by the extended Euclidean algorithm it is possible to find k such that

$$e_A d_A = 1 + k\phi_A = 1 + k(p_A - 1)(q_A - 1.$$

(Run Extended Euclidean algorithm on $(e_A, \phi(n_A))$ or $(d_A, \phi(n_A))$.)
From Fermat' theorem we get,

$$M^{p_A - 1} \equiv 1 \ (mod \ p_A).$$

Hence,

$$M^{e_A d_A} \equiv M^{1+k(p_A-1)(q_A-1)} \equiv M \ (M^{(p_A-1)})^{(q_A-1)} \equiv M \ (mod \ p_A).$$

Similarly,

$$M^{e_A d_A} \equiv M^{1+k(p_A-1)(q_A-1)} \equiv M \ (M^{(q_A-1)})^{(p_A-1)} \equiv M \ (mod \ q_A).$$

Since, p_A and q_A are distinct primes, it follows from Chinese Remainder Theorem that

$$M^{e_A\ d_A} \equiv M\ (mod\ \ n_A).$$

This implies,

$$c^{d_A} = (M^{e_A})^{d_A} \equiv M\ (mod\ \ n_A).$$

More serious proof of RSA Decryption

Note that we need to prove

$$(M^{e_A})^{d_a} = M^{e_A\ d_A} = M\ mod\ n_A.$$

If M is relatively prime to n_A, then this implies $(M, p_A) = (M, q_A) = 1$. Then the arguments in the previous slides prove the result.
You can also see this as an application of Eulers's theorem. Note that,

$$e_A d_A = 1 + k\phi_A = 1 + k(p_A - 1)(q_A - 1). \qquad (1)$$

Then

$$M^{e_A\ d_A} = M^{1+k\phi_A} = M\ M^{k\phi_A} = M\ (M^{\phi_A})^k = M$$

as $M^{\phi_A} = 1\ mod\ n_A$ (Eulers's theorem).
However, again note that to be able to use Fermat's or Euler's theorem, we need $(M, n_A) = 1$.

What if M is not relatively prime to n?

Note that the probability that M is not relatively prime to n_A is very small $(1/p_A + 1/q_A - 1/(p_A q_A))$. If we just ignore this possibility we are done. But, if you are serious and want to prove the RSA result for all $M < n_A$, then see the following.

Case when M is not relatively prime to n_A.

In this case M is divisible by either p_A or q_A. If it is divisible by both p_A and q_A, then $M = \ 0 \ mod \ n_A$ and hence the RSA result is trivially true. Then with out loss of generality assume that p_A divides M and hence we can write $M = c \ p_A$. Then we must have $(M, q_A) = 1$ (Otherwise, M is also multiple of q_A and hence identically equal to $0 \ mod \ n_A$).

Now we can use Fermat's theorem

$$M^{(q_A - 1)} = 1 \ mod \ q$$

Then taking $(k(p_A - 1))^{th}$ power on either side of the above equation, we get,

$$M^{k(p_A-1)(q_A-1)} = 1 \ mod \ q_A,$$

where k is as in (1). This implies

$$M^{k(p_A-1)(q_A-1)} = 1 + k' \ q_A.$$

Multiplying each side by $M = cp_A$, we get

$$M^{k(p_A-1)(q_A-1)+1} = M + k' \ c \ p_A \ q_A = M + k'' \ n_A.$$

Taking $mod \ n_A$ on both sides gives the result.