Week 2

Lecture 2

Properties of Numbers II

University of Melbourne

Week 2

Lecture 1

- Part -1 Extended GCD Algorithm and Related Computations
- Part -2 Symmetric key Cryptography

Lect

Properties of Numbers

Workshop 2: Workshops start from this week

Quizz 2

2.1

2.2

2.3

2.1

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

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

if a and b differ by a multiple of n; i.e ; if n is a factor of $b \;\; - a|$.
Ever

the se

We can define the following operations:

$$x \oplus_n y = (x + y)$$

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

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 Z_n, if there is an integer y such that

then

$y = x^{-1}$ *usually.*

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

Determining multiplicative inverse

Fact

For an *hat*

You can determine x and y by modifyin $gcd(a, b)$. Thus we can say that we can find inverse o lo b provided $gcd(a, b) = 1$.

2.2

Euler Phi function

Definition

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

Definition

Eule $\phi(n)$
deno *me*
to n.

Definition

Reduced set of residues mod n: For n
residues, $R(n)$ is defined as set of residues mod
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

for an

Consider numbers from 0 to $p^a - 1$, the

some common divisor with p^a are those n

multiple of p. There are exactly p^{a-1}

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 ex q to form

)

In the above counting, we have excluded multiple ce while excluding the multiples of p and a multiples of q. So we need to make the following c

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

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

But t

num

Using the above fact, we can derive a general result a ϕ function. We know that any number has a unique fa

$$n = \Pi_{i=1}^{\tau} p_i^{a_i} = p_1^{a_1}\ p$$

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:

Fro

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

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

2.3

Inverse Mod n again

We have seen how Extended GCD Algorithm to compute *inverse*(a) / mod n before.

We wi

$\mathbf{Z}_n^\star$ b

The

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

Now, how can you use the above theorem for compu

$a \mod n$?

$inverse(a) \mod n$

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

Lect

Properties of Numbers

Workshop 2: Workshops start from this week

Quizz 2