Day 4

Discrete Mathematics

Number theory

Dr. Abhijit Debnath

University of Engineering and Management

Reference book for this material is

Rosen, K. H., & Krithivasan, K. (1999). *Discrete mathematics and its applications* (Vol. 6). New York: McGraw-hill.

Prime

An integer p greater than 1 is called *prime* if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called *composite.*

The integer 7 is prime because its only positive factors are 1 and 7, whereas the integer 9 is composite because it is divisible by 3.

THE FUNDAMENTAL THEOREM OF ARITHMETIC

Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

- If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Proof: If n is composite, by the definition of a composite integer, we know that it has a factor a with $1 < a < n$. Hence, by the definition of a factor of a positive integer, we have $n = ab$, where b is a positive integer greater than 1. We will show that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. If $a > \sqrt{n}$ and $b > \sqrt{n}$, then $ab > \sqrt{n} \cdot \sqrt{n} = n$, which is a contradiction. Consequently, $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.
Because both a and b are divisors of n, we see that n has a positive divisor not exceeding $\sqrt{n}$. This divisor is either prime or, by the fundamental theorem of arithmetic, has a prime divisor less than itself. In either case, n has a prime divisor less than or equal to $\sqrt{n}$.

❖ There are infinitely many primes.

Proof: We will prove this theorem using a proof by contradiction. We assume that there are only finitely many primes, $p1, p2, \ldots, pn$. Let, $Q= p1p2\cdot \cdot \cdot pn + 1$.

By the fundamental theorem of arithmetic, Q is prime or else it can be written as the product of two or more primes. However, none of the primes pj divides Q, for if $pj \mid Q$, then $pjQ- p1p2\cdot \cdot \cdot pn = 1$. Hence, there is a prime not in the list $p1, p2, \ldots, pn$. This prime is either Q, if it is prime, or a prime factor of Q. This is a contradiction because we assumed that we have listed all the primes. Consequently, there are infinitely many primes.

Congruent modulo

Theorem:

Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Proof: If $a \equiv b \pmod{m}$, by the definition of congruence (Definition 3), we know that $m \mid (a - b)$. This means that there is an integer k such that $a - b = km$, so that $a = b + km$.
Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$. Hence, m divides $a - b$, so that $a \equiv b \pmod{m}$.

Congruent modulo

Theorem:

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Proof: We use a direct proof. Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, by Theorem 4 there are integers s and t with $b = a + sm$ and $d = c + tm$. Hence, $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$

and

$bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$.

Hence, $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Congruent modulo

1. What are the quotient and remainder when
a) 19 is divided by 7?
b) -111 is divided by 11?
c) 789 is divided by 23?
d) 1001 is divided by 13?
e) 0 is divided by 19?
f) 3 is divided by 5?
g) -1 is divided by 3?
h) 4 is divided by 1?
2. What are the quotient and remainder when
a) 44 is divided by 8?
b) 777 is divided by 21?
c) -123 is divided by 19?
d) -1 is divided by 23?
e) -2002 is divided by 87?
f) 0 is divided by 17?
g) 1,234,567 is divided by 1001?
h) -100 is divided by 101?

Congruent modulo

Suppose that a and b are integers, $a \equiv 11 \pmod{19}$, and $b \equiv 3 \pmod{19}$. Find the integer c with $0 \leq c \leq 18$ such that

a) $c \equiv 13a \pmod{19}$.

b) $c \equiv 8b \pmod{19}$.

c) $c \equiv a - b \pmod{19}$.

d) $c \equiv 7a + 3b \pmod{19}$.

e) $c \equiv 2a2 + 3b2 \pmod{19}$.

f) $c \equiv a3 + 4b3 \pmod{19}$.

Congruent modulo

Evaluate these quantities.

a)-17 **mod** 2 **c)**-101 **mod** 13 **b)** 144 **mod** 7

d) 199 **mod** 19

Evaluate these quantities.

a) 13 **mod** 3 **c)** 155 **mod** 19 **b)**-97 **mod** 11

d)-221 **mod** 23

UEM
श्रद्धावान लभते ज्ञानम्
UNIVERSITY OF ENGINEERING & MANAGEMENT
Good Education, Good Jobs

Congruent modulo

Evaluate these quantities.

a)-17 **mod** 2 **c)**-101 **mod** 13 **b)** 144 **mod** 7

d) 199 **mod** 19

Evaluate these quantities.

a) 13 **mod** 3 **c)** 155 **mod** 19 **b)**-97 **mod** 11

d)-221 **mod** 23

Thank you