CS311H: Discrete Mathematics

Introduction to Number Theory

Instructor: Işıl Dillig

Introduction to Number Theory

- Number theory is the branch of mathematics that deals with integers and their properties
- Number theory has a number of applications in computer science, esp. in modern cryptography in cryptography

Divisibility

- Given two integers a and b where $a \neq 0$, we say a divides b if there is an integer c such that $b = ac$
- If a divides b, we write $a|b$; otherwise, $a \not| b$
- Example: $2|6$, $2 \not| 9$
- If $a|b$, a is called a factor of b
- b is called a multiple of a

Example

- Question: If n and d are positive integers, how many positive integers not exceeding n are divisible by d?
- Recall: All positive integers divisible by d are of the form dk
- We want to find how many numbers dk there are such that $0 < dk \leq n$.
- In other words, we want to know how many integers k there are such that $0 < k \leq \frac{n}{d}$
- How many integers are there between 1 and $\frac{n}{d}$?

Properties of Divisibility

- Theorem 1: If $a|b$ and $b|c$, then $a|c$
-
-
-
-

Divisibility Properties, cont.

- Theorem 2: If $a|b$ and $a|c$, then $a|(mb + nc)$ for any int m, n
- Proof:
- Corollary 1: If $a|b$ and $a|c$, then $a|(b + c)$ for any int c
- Corollary 2: If $a|b$, then $a|mb$ for any int m

The Division Theorem

- Division theorem: Let a be an integer, and d a positive integer. Then, there are unique integers q, r with $0 \leq r < d$ such that $a = dq + r$
- Here, d is called divisor, and a is called dividend
- q is the quotient, and r is the remainder.
- We use the $r = a \bmod d$ notation to express the remainder
- The notation $q = a \text{ div } d$ expresses the quotient
- What is $101 \bmod 11$?
- What is $101 \text{ div } 11$?

Congruence Modulo

- In number theory, we often care if two integers a, b have same remainder when divided by m.
- If so, a and b are congruent modulo m, $a \equiv b \pmod{m}$.
- More technically, if a and b are integers and m a positive integer, $a \equiv b \pmod{m}$ iff $m | (a - b)$
- Example: 7 and 13 are congruent modulo 3.
- Example: Find a number congruent to 7 modulo 4.

Congruence Modulo Theorem

- Theorem: $a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$
- Part 1, $\Rightarrow$: Suppose $a \equiv b \pmod{m}$.
- Then, by definition of $\equiv$, $m|(a - b)$
- By definition of $|$, there exists k such that $a - b = mk$, i.e., $a = b + mk$
- By division thm, $b = mp + r$ for some $0 \leq r < m$
- Then, $a = mp + r + mk = m(p + k) + r$
- Thus, $a \bmod m = r = b \bmod m$

Congruence Modulo Theorem Proof, cont.

- Theorem: $a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$
- Part 2, $\Leftarrow$: Suppose $a \bmod m = b \bmod m$
- Then, there exists some p_1, p_2, r such that $a = p_1 \cdot m + r$ and $b = p_2 \cdot m + r$ where $0 \leq r < m$
- Then, $a - b = p_1 \cdot m + r - p_2 \cdot m - r = m \cdot (p_1 - p_2)$
- Thus, $m|(a - b)$
- By definition of $\equiv$, $a \equiv b \pmod{m}$

Example

- Prove that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then:

$$a + c \equiv b + d \pmod{m}$$

-
-
-
-
-

Applications of Congruence in Cryptography

- Congruences have many applications in cryptography, e.g., shift ciphers
- Shift cipher with key k encrypts message by shifting each letter by k letters in alphabet (if past Z, then wrap around)
- What is encryption of "KILL HIM" with shift cipher of key 3?
- Shift ciphers also called Ceasar ciphers because Julius Ceasar encrypted secret messages to his generals this way

Mathematical Encoding of Shift Ciphers

- First, let's number letters A-Z with $0 - 25$
- Represent message with sequence of numbers
- Example: The sequence "25 0 2" represents "ZAC"
- To encrypt, apply encryption function f defined as:

$$f(x) = (x + k) \bmod 26$$

- Because f is bijective, its inverse yields decryption function:

$$g(x) = (x - k) \bmod 26$$

Ciphers and Congruence Modulo

- Shift cipher is a very primitive and insecure cipher because very easy to infer what k is
- But contains some useful ideas:
  - Encoding words as sequence of numbers
  - Use of modulo operator
- Modern encryption schemes much more sophisticated, but also share these principles (coming lectures)

Prime Numbers

- A positive integer p that is greater than 1 and divisible only by 1 and itself is called a prime number.
- First few primes: $2, 3, 5, 7, 11, \ldots$
- A positive integer that is greater than 1 and that is not prime is called a composite number
- Example: $4, 6, 8, 9, \ldots$

Fundamental Theorem of Arithmetic

- Fundamental Thm: Every positive integer greater than 1 is either prime or can be written uniquely as a product of primes.
- This unique product of prime numbers for x is called the prime factorization of x
- Examples:
  - $12 =$
  - $21 =$
  - $99 =$

Determining Prime-ness

- In many applications, such as crypto, important to determine if a number is prime – following thm is useful for this:
- Theorem: If n is composite, then it has a prime divisor less than or equal to $\sqrt{n}$
-
-
-
-

Consequence of This Theorem

Theorem: If n is composite, then it has a prime divisor $\leq \sqrt{n}$

- Thus, to determine if n is prime, only need to check if it is divisible by primes $\leq \sqrt{n}$
- Example: Show that 101 is prime
- Since $\sqrt{101} < 11$, only need to check if it is divisible by $2, 3, 5, 7$.
- Since it is not divisible by any of these, we know it is prime.

Infinitely Many Primes

- Theorem: There are infinitely many prime numbers.
- Proof: (by contradiction) Suppose there are finitely many primes: $p_1, p_2, \ldots, p_n$
- Now consider the number $Q = p_1 p_2 \ldots p_n + 1$. Q is either prime or composite
- Case 1: Q is prime. We get a contradiction, because we assumed only prime numbers are $p_1, \ldots, p_n$
- Case 2: Q is composite. In this case, Q can be written as product of primes.
- But Q is not divisible by any of $p_1, p_2, \ldots, p_n$
- Hence, by Fundamental Thm, not composite $\Rightarrow \perp$ $\square$