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
- Next few lectures: Basic concepts in number theory and its application in crypto

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, $a \nmid b$
- Example: $2|6$, $2 \nmid 9$
- 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 $\Rightarrow \perp$ $\square$

Greatest Common Divisors

- Suppose a and b are integers, not both 0.
- Then, the largest integer d such that $d|a$ and $d|b$ is called greatest common divisor of a and b, written gcd(a,b).
- Example: gcd$(24, 36) =$
- Example: gcd$(2^3 5, 2^2 3) =$
- Example: gcd$(14, 25) =$
- Two numbers whose gcd is 1 are called relatively prime.
- Example: 14 and 25 are relatively prime

Least Common Multiple

- The least common multiple of two positive integers a and b, written lcm(a,b), is the smallest integer c such that $a|c$ and $b|c$.
- Example: lcm$(9, 12)$=
- Example: lcm$(2^3 3^5 7^2, 2^4 3^3)$=

Theorem about LCM and GCD

- Theorem: Let a and b be positive integers. Then, $ab = \text{gcd}(a, b) \cdot \text{lcm}(a, b)$
- Proof: Let $a = p_1^{i_1} p_2^{i_2} \ldots p_n^{i_n}$ and $b = p_1^{j_1} p_2^{j_2} \ldots p_n^{j_n}$
- Then, $ab = p_1^{i_1+j_1} p_2^{i_2+j_2} \ldots p_n^{i_n+j_n}$
- $\text{gcd}(a, b) = p_1^{min(i_1,j_1)} p_2^{min(i_2,j_2)} \ldots p_n^{min(i_n,j_n)}$
- $\text{lcm}(a, b) = p_1^{max(i_1,j_1)} p_2^{max(i_2,j_2)} \ldots p_n^{max(i_n,j_n)}$
- Thus, we need to show $i_k + j_k = min(i_k, j_k) + max(i_k, j_k)$

Proof, cont.

- Show $i_k + j_k = min(i_k, j_k) + max(i_k, j_k)$

Computing GCDs

- Simple algorithm to compute gcd of a, b:
  - Factorize a as $p_1^{i_1} p_2^{i_2} \ldots p_n^{i_n}$
  - Factorize b as $p_1^{j_1} p_2^{j_2} \ldots p_n^{j_n}$
  - $\text{gcd}(a, b) = p_1^{min(i_1,j_1)} p_2^{min(i_2,j_2)} \ldots p_n^{min(i_n,j_n)}$
- But this algorithm is not good because prime factorization is computationally expensive! (not polynomial time)
- Much more efficient algorithm to compute gcd, called the Euclidian algorithm

Insight Behind Euclid's Algorithm

- Theorem: Let $a = bq + r$. Then, $\gcd(a, b) = \gcd(b, r)$
- e.g., Consider $a = 12$, $b = 8$ and $a = 12, b = 5$
- Proof: We'll show that a, b and b, r have the same common divisors – implies they have the same gcd.

$\Rightarrow$ Suppose d is a common divisor of a, b, i.e., $d|a$ and $d|b$

- By theorem we proved earlier, this implies $d|a - bq$
- Since $a - bq = r$, $d|r$. Hence d is common divisor of b, r.

$\Leftarrow$ Now, suppose $d|b$ and $d|r$. Then, $d|bq + r$

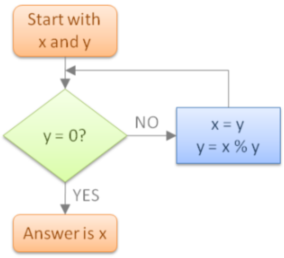
- Hence, $d|a$ and d is common divisor of a, b $\square$

Using this Theorem

Theorem: Let $a = bq + r$. Then, $\gcd(a, b) = \gcd(b, r)$

- Suggests following recursive strategy to compute gcd(a, b):
  - Base case: If b is 0, then gcd is a
  - Recursive case: Compute gcd(b, a $\bmod$ b)
- Claim: We'll eventually hit base case – why?

Euclidian Algorithm



- Find gcd of 72 and 20
- $12 = 72\%20$
- $8 = 20\%12$
- $4 = 12\%8$
- $0 = 8\%4$
- gcd is 4!

GCD as Linear Combination

- gcd(a, b) can be expressed as a linear combination of a and b
- Theorem: If a and b are positive integers, then there exist integers s and t such that:

$$\gcd(a, b) = s \cdot a + t \cdot b$$

- Furthermore, Euclidian algorithm gives us a way to compute these integers s and t (known as extended Euclidian algorithm)

Example

- Express $\gcd(72, 20)$ as a linear combination of 72 and 20
- First apply Euclid's algorithm (write $a = bq + r$ at each step):
  1. $72 = 3 \cdot 20 + 12$
  2. $20 = 1 \cdot 12 + 8$
  3. $12 = 1 \cdot 8 + 4$
  4. $8 = 2 \cdot 4 + 0 \Rightarrow$ gcd is 4
- Now, using (3), write 4 as $12 - 1 \cdot 8$
- Using (2), write 4 as $12 - 1 \cdot (20 - 1 \cdot 12) = 2 \cdot 12 - 1 \cdot 20$
- Using (1), we have $12 = 72 - 3 \cdot 20$, thus:

$$4 = 2 \cdot (72 - 3 \cdot 20) - 1 \cdot 20 = 2 \cdot 72 + (-7) \cdot 20$$

Exercise

Use the extended Euclid algorithm to compute $\gcd(38, 16)$.

A Useful Result

- Lemma: If a, b are relatively prime and $a|bc$, then $a|c$.
- Proof: Since a, b are relatively prime $\gcd(a, b) = 1$
- By previous theorem, there exists s, t such that $1 = s \cdot a + t \cdot b$
- Multiply both sides by c: $c = csa + ctb$
- By earlier theorem, since $a|bc$, $a|ctb$
- Also, by earlier theorem, $a|csa$
- Therefore, $a|csa + ctb$, which implies $a|c$ since $c = csa + ctb$ $\square$

Example

Lemma: If a, b are relatively prime and $a|bc$, then $a|c$.

- Suppose $15 \mid 16 \cdot x$
- Here 15 and 16 are relatively prime
- Thus, previous theorem implies: $15|x$

Question

- Suppose $ca \equiv cb \pmod{m}$. Does this imply $a \equiv b \pmod{m}$?

Another Useful Result

- Theorem: If $ca \equiv cb \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$

Examples

- If $15x \equiv 15y \pmod{4}$, is $x \equiv y \pmod{4}$?
- If $8x \equiv 8y \pmod{4}$, is $x \equiv y \pmod{4}$?