Discrete Mathematics

Set 5: Number Theory

NYU, Abu Dhabi,
Spring 2020

Introduction and Definitions

Introduction

- Number theory is the branch of mathematics that deals with integers and their properties
- Number theory has a number of applications in computer science, especially in modern 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 $a \mid b$; otherwise, $a \nmid b$
- Example: $5 \mid 10$; but, $5 \nmid 12$
- If $a \mid b$, a is called a factor of b, and then 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 $a \mid b$ and $b \mid c$, then $a \mid c$.
  Proof: on the whiteboard.

- Theorem 2: if $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ for any integers m, n.
  Proof: on the whiteboard.

- Corollary 1: If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
  Proof: try it

- Corollary 2: If $a \mid b$ then $a \mid mb$ for any integer m
  Proof: try it

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 notation $r = a \; mod \; d$ to express the remainder,
- We use the notation $q = a \; div \; d$ expresses the quotient.

- What is 105 mod 11?
- What is 105 div 11?

The Congruence Modulo

Congruence Modulo

- In number theory, we often care if two integers a, b have the same remainder when divided by m.
- If so, we say that a and b are congruent modulo m, and we write $a \equiv b (mod\, m)$.
- More technically, if a and b are integers and m a positive integer, then $a \equiv b (mod\, m)$ iff $m \mid (a - b)$

- Example: 7 and 13 are congruent modulo 3.
- Example: Find a number congruent to 7 modulo 4.

Congruence Modulo Theorem

- Theorem: $a \equiv b(mod\ m)$ iff $a\ mod\ m = b\ mod\ m$
- Proof: to be done in 2 parts $\Longrightarrow$ and $\Longleftarrow$
- Part 1, $\Longrightarrow$
  - Suppose $a \equiv b(mod\ m)$, show that $a\ mod\ m = b\ mod\ m$,
  - if $a \equiv b(mod\ m)$, then by definition of $\equiv$, we have $m \mid (a - b)$
  - By definition of $\mid$, there exists k such that $a - b = mk$, i.e., $a = b + mk$
  - By division theorem, $b = mp + r$ for some $0 \leq r < m$
  - Then, $a = mp + r + mk = m(p + k) + r$
  - Thus, $a\ mod\ m = r = b\ mod\ m$
- Part 2, $\Longleftarrow$
  - Suppose $a\ mod\ m = b\ mod\ m$, show that $a \equiv b(mod\ m)$
  - if $a\ mod\ m = b\ mod\ m$, then, there exists some p_1, p_2, r such that $a = p_1 m + r$ and $b = p_2 m + r$ where $0 \leq r < m$
  - Then, $a - b = p_1 m + r - p_2 m - r = m(p_1 - p_2)$
  - Thus, $m \mid (a - b)$, and hence by definition of $\equiv$, we have $a \equiv b(mod\ m)$

Congruence Modulo: Example

- Prove that if $a \equiv b (mod\ m)$ and $c \equiv d (mod\ m)$, then $a + c \equiv b + d\ (mod\ m)$
- Proof: on the whiteboard.

Applications of Congruence in Cryptography

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 "GO FOR PEACE" with shift cipher of key 3?
- Shift ciphers also called Ceasar ciphers because Julius Ceasar encrypted secret messages to his generals this way

Applications of Congruence in Cryptography

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:

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

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

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

Applications of Congruence in Cryptography

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

Prime vs Composite 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, . . .
- A positive integer that is greater than 1 and that is not prime is called a composite number
- Example: 4, 6, 8, 9, . . .

Fundamental Theorem of Arithmetic

- Fundamental Theorem: Every positive integer greater than 1 is either prime or can be written uniquely as a product of primes.
- Proof: See the proof of this theorem in slide 17 of the proofs lecture (section proof by induction).
- 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, it is important to determine if a number is prime. The following theorem is useful for determining primeness.

- Theorem: if $n \in \mathbb{N} > 1$ is composite, then $\exists\, 1 < m \in \mathbb{N} \leq \sqrt{n}$ such that $m \mid n$.
- This means: If n is composite, then it has a prime divisor less than or equal to to $\sqrt{n}$
- Proof: on the whiteboard (by contradiction)
- 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 $\sqrt{n} < 11$, we only need to check if 101 is divisible by $2, 3, 5, 7$.
  - Since it is not divisible by any of these, we know it is prime.

The set of primes is infinite

- Theorem: There are infinitely many prime numbers.
- Proof: on whiteboard (by contradiction)

More about Cryptography

Modern cryptography, which is based on encoding a message with the use of a "key" made public (!!), is based on the following fact:

- It is fairly easy to find very large prime numbers, but it is hard to factor a composite number.

- The "easy" algorithms that look for primes do not reject composites by factoring them, but by using other number-theoretic criteria.

- A very important theorem in this respect was discovered fairly recently by a relatively unknown mathematician in India and two of his undergraduate (!) students (Agrawal–Kayal–Saxena, AKS, primality test, 2002).

Cryptography deciphered

The public key cryptography works by

- Finding large primes (fairly easy as noted),
- Multiplying them to get a composite, and then
- Making the product public to be used as a cryptographic key.
- Deciphering, on the other hand resides on knowing the two prime factors of the composite, that isn't easy to find,
- but are known to the receiver of the message, who generated the key in the first place.
- Naturally, the receiver takes care to change often the public key, just in case!

Greatest Common Divisor

Definition

Given non-zero integers $a, b \in \mathbb{Z}$, their greatest common divisor, notationally $\gcd(a, b)$, is the largest positive integer that divides both a, b.

Theorem

If $a, b \in \mathbb{Z}$ are two non-zero integers and $a \neq b$, then $\gcd(a, b) = \gcd(a - b, b)$.

Proof: *By the properties of divisibility of the sum..*

Lemma

Let $a, b \in \mathbb{N}$ where $b \neq 0$, and let $a = bq + r$ where $0 \leq r < b$ then $\gcd(a, b) = \gcd(b, r)$.

Proof: *On the whiteboard.*

The Wisdom of Quotes

Real Mathematics ... is almost wholly useless

– "A Mathematician's Apology", 1940, G. H. Hardy
(a distinguished researcher with important contributions in Number Theory).

Euclid's algorithm, 4th century BCE

To find the gcd(a, b) of two positive unequal integers,

- Replace the largest with its difference form the other.
- Repeat until they become equal, or one of the numbers becomes 1.

- The correctness is based on the previous theorem.

EXAMPLE

Try to compute gcd$(13, 199)$

Observation

Observe that it pays to replace the operation $a - b$ with $a \bmod b$. If this results to generating 0 during the process, then one of the numbers divides the other, so the gcd is the smallest.

More from Euclid

If in the process of executing Euclid's algorithm, we keep track of the subtractions performed, we get:

Theorem

For any two non-zero integers a, b, there exist integers x, y (not necessarily positive) such that $\gcd(a, b) = xa + yb$. Moreover, the x, y can be algorithmically computed.

Definition

Two non-zero integers are called relatively prime if $\gcd(a, b) = 1$

Corollary

If a, b are relatively prime then $\exists x, y \in \mathbb{Z}$ s.t. $1 = xa + yb$.

More about "modula"

Theorem

Given relatively prime integers $a, m > 1$ then the equation $ax \equiv b \mod m$ has a solution in $x \in \{1, \ldots, m\}$, $\forall b \in \mathbb{Z}$ and $b \neq 0$.

Proof.

By the previous corollary $\exists x, y \in \mathbb{Z}$ such that $1 = xa + ym$. Observe that $x \neq 0$. Multiply both sides by b to get $abx = b - bym$. Therefore $a(bx) \equiv b \mod m$. To get a solution in $\{1, \ldots, m\}$, take $bx \mod m$. □

Even more about "modula"

Corollary

If p is a prime, every non-zero integer a is invertible $\mod p$, meaning that there is an integer b such that $ab \equiv 1 \mod p$

Proof.

Apply previous theorem for $m = p$ and $b = 1$. □

Remark

The importance of the above corollary is that when doing arithmetic modulo a prime, we can invert a non-zero number, and therefore we can factor it out as well.

Primality testing and Fermat's little theorem

Theorem (Fermat, 17th century CE)

If p is prime, then for every $1 \leq a < p$, $a^{p-1} \equiv 1 \bmod p$.

- The inverse of the above theorem is not true, as taking $p = 341, a = 2$ testifies.
- Yet if we get that indeed $a^{p-1} \equiv 1 \bmod p$, for many judiciously chosen a, we can conclude that the probability that p is prime very high.
- This led the way to efficient, but randomized, primality checks that do not necessitate looking for factors of p.
- As noted, the AKS test offers an efficient, and factorless, deterministic criterion.

Proof of Fermat's little theorem

Proof.

By definition of the $\mod$ operation,

$$\{(a \cdot 1 \mod p), \ldots, (a \cdot (p-1) \mod p)\} \subseteq \{1, \ldots, p-1\} \quad (1)$$

Now observe that $(a \cdot 1 \bmod p), \ldots, (a \cdot (p-1) \bmod p)$ are pairwise distinct. Indeed if $a \cdot i \equiv a \cdot j \bmod p$ for some $1 \leq i < j < p$, we can factor out a, to get that $i \equiv j \bmod p$, a contradiction. Therefore the two sets in (1) have equal cardinality, so they are equal. Taking the product of all elements of both, we get: $a^{p-1}(p-1)! \equiv (p-1)! \bmod p$. But easily $p-1$ is not $\equiv 0 \bmod p$, so $(p-1)!$ can be factored out of the equality $a^{p-1}(p-1)! \equiv (p-1)! \bmod p$ to get the required. □