CS311H: Discrete Mathematics  

Number Theory  

Instructor: İslil Dillig  

---  

Announcements  

- Midterm grades posted on Canvas  
- Mean: 47/65 (72%)  
- Standard deviation: 9  
- Talk with me if you are concerned about grade!  

---  

Number Theory Review  

- What does it mean for two ints $a, b$ to be congruent mod $m$?  
- What is the Division theorem?  
- If $a | b$ and $a | c$, does it mean $b | c$?  

---  

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, 
- 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 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  

- 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: \( p_1, p_2, ..., p_n \)
  - Now consider the number \( Q = p_1 p_2 ... p_n + 1 \). \( Q \) is either prime or composite
  - **Case 1:** \( Q \) is prime. We get a contradiction, because we assumed only prime numbers are \( p_1, ..., p_n \)
  - **Case 2:** \( Q \) is composite. In this case, \( Q \) can be written as product of primes.
    - But \( Q \) is not divisible by any of \( p_1, p_2, ..., p_n \)
    - Hence, by Fundamental Thm, not composite ⇒ \( \bot \)

A Word about Prime Numbers and Cryptography

- Prime numbers play a key role in modern cryptography – rely on prime numbers to encrypt messages
- Security of encryption relies on prime factorization being intractable for sufficiently large numbers
- More on this later!

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:** \( \gcd(24, 36) = 12 \)
  - **Example:** \( \gcd(2^35^2, 2^33) = 8 \)
  - **Example:** \( \gcd(14, 25) = 1 \)
  - 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 \( a \) and \( b \), written \( \lcm(a, b) \), is the smallest integer \( c \) such that \( a | c \) and \( b | c \).
- **Example:** \( \lcm(9, 12) = 36 \)
  - **Example:** \( \lcm(2^33^57^2, 2^33^3) = 936 \)

Theorem about LCM and GCD

- **Theorem:** Let \( a \) and \( b \) be positive integers. Then, \( ab = \gcd(a, b) \cdot \lcm(a, b) \)
  - Proof: Let \( a = p_1^{i_1}p_2^{i_2}...p_k^{i_k} \) and \( b = p_1^{j_1}p_2^{j_2}...p_k^{j_k} \)
  - Then, \( ab = p_1^{i_1+j_1}p_2^{i_2+j_2}...p_k^{i_k+j_k} \)
  - \( \gcd(a, b) = p_1^{\min(i_1,j_1)}p_2^{\min(i_2,j_2)}...p_k^{\min(i_k,j_k)} \)
  - \( \lcm(a, b) = p_1^{\max(i_1,j_1)}p_2^{\max(i_2,j_2)}...p_k^{\max(i_k,j_k)} \)
  - 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 $p_1^{j_1} p_2^{j_2} \ldots p_n^{j_n}$
  - $\gcd(a, b) = p_1^{\min(i_1, j_1)} p_2^{\min(i_2, j_2)} \ldots p_n^{\min(i_n, j_n)}$
  - 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.
    - 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 $b, r$.
    - Now, suppose $d | b$ and $d | r$. Then, $d | bq + r$
    - Hence, $d | a$ and $d$ is common divisor of $a, b$

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 $\gcd(b, a \mod b)$
  - 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!

Euclidian Algorithm Example

- Find gcd of 662 and 414
  - $248 = 662 \% 414$
  - $166 = 414 \% 248$
  - $82 = 248 \% 166$
  - $2 = 166 \% 82$
  - $0 = 82 \% 2$
  - gcd is 2!
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, Euclidean algorithm gives us a way to compute these integers \( s \) and \( t \) (known as extended Euclidean 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 \( a \mid bc \), then \( a \mid c \).
- **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 \( a \mid bc, a \mid cb \)
  - Also, by earlier theorem, \( a \mid csa \)
  - Therefore, \( a \mid csa + ctb \), which implies \( a \mid c \) since \( c = csa + ctb \)

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 \( x \equiv y \pmod{4} \)?