Announcements

- Midterms are graded – scores on Blackboard
  - Graded midterms handed back at the end of class
  - Make sure score on midterm matches grade on Blackboard
  - If not, let us know asap (within a week at latest)
- Sample solutions posted on course webpage – look over them!
- Since only 1-2 students answered Question (4c) correctly and since there was small typo, did not count (4c) when calculating grades – thus, grades out of 80 rather than 90

Announcements, cont.

- Average on midterm 55 out of 80; standard deviation is 17
- Third homework also graded – scores on Blackboard
- Average on HW3 is 67 out of 100

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, esp. in modern cryptography
- This lecture: Important results in number theory
- Next lecture: Continue discussion of number theory, look at applications of number theory 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, $a \nmid b$
- Example: $2 | 6, 2 \nmid 9$
- If $a | b$, $a$ is called a factor of $b$
- $b$ is called a multiple of $a$
- All integers divisible by $a$ can be enumerated as: $\ldots, -3a, -2a, -a, 0, a, 2a, 3a, \ldots$

Example

- Question: If $n$ and $d$ are positive integers, how many 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 $a|c$, then $a|(b + c)$
- **Proof**: If $a|b$, there exists $k_1$ such that $b = ak_1$
  - Similarly, if $a|b$, then $k_2$ such that $c = ak_2$
  - Then, $b + c = a(k_1 + k_2)$
  - Hence, $a|(b + c)$

More Divisibility Properties

- **Theorem 4**: If $a|b$ and $a|c$, then $a|(mb + nc)$
  - **Proof**: By Thm 2, if $a|b$, then $a|mb$
  - By thm 2, if $a|c$, then $a|nc$
  - Therefore, $a|(mb + nc)$

Divisibility Properties, cont.

- **Theorem 3**: If $a|b$ and $b|c$, then $a|c$
- **Proof**: If $a|b$, there exists $k_1$ such that $b = ak_1$
  - Hence, $a|c$. 

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 $r = a \mod d$ notation to express the remainder
  - The notation $q = a \div d$ expresses the quotient
  - What is $101 \mod 11$?
  - What is $101 \div 11$?

Congruence Modulo

- Sometimes, we care if two integers $a, b$ have the same remainder when divided by some number $m$.
  - 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 $a \mod m = b \mod m$
- **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, $a \mod m = r = b \mod m$

In this section, we have discussed congruences in the context of shift ciphers. Shift ciphers are a very primitive and insecure cipher because it is very easy to infer what $k$ is.

**Applications of Congruence in Cryptography**

- Congruences have many applications in cryptography
- For instance, Julius Caesar encrypted messages by shifting each letter three letters in the alphabet ("Caesar cipher")
- For example, the message "I LIKE DISCRETE MATH" would be encrypted as "L OLNH GLYFUHVH PDVK"
- Caesar’s cipher example of shift cipher: shifts each letter by $k$
- For Caesar cipher, $k = 3$
- We can express shift ciphers using the modulo operator

**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:
  $$f^{-1}(x) = (x - k) \mod 26$$

Shift ciphers are a very primitive and insecure cipher because it is 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
- More on this next lecture!
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, …

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 \( \sqrt{n} \)
  - **Proof**: Since \( n \) is composite, it can be written as \( n = ab \) where \( a > 1 \) and \( b > 1 \).
  - For contradiction, suppose neither \( a \) nor \( b \) are \( \leq \sqrt{n} \), i.e., \( a > \sqrt{n} \) and \( b > \sqrt{n} \).
  - Then, \( n = ab > \sqrt{n} \cdot \sqrt{n} = n \), a contradiction.
  - Hence, either \( a \leq \sqrt{n} \) or \( b \leq \sqrt{n} \), and by the Fundamental Thm, is either itself a prime or has a factor less than itself.

Infinately 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 \( Q = p_1 p_2 \cdots p_n + 1 \). \( Q \) 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 \( \Rightarrow \bot \).

Consequence of This Theorem

- **Theorem**: If \( n \) is composite, then it has a prime divisor \( \leq \sqrt{n} \)
  - **Proof**: Since \( n \) is composite, it can be written as \( n = ab \) where \( a > 1 \) and \( b > 1 \).
  - For contradiction, suppose neither \( a \) nor \( b \) are \( \leq \sqrt{n} \), i.e., \( a > \sqrt{n} \) and \( b > \sqrt{n} \).
  - Then, \( n = ab > \sqrt{n} \cdot \sqrt{n} = n \), a contradiction.
  - Hence, either \( a \leq \sqrt{n} \) or \( b \leq \sqrt{n} \), and by the Fundamental Thm, is either itself a prime or has a factor less than itself.

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.
- **Examples**: 12, 21, 99

A Word about Prime Numbers and Cryptography

- Prime numbers play a key role in modern cryptography
- Modern cryptography techniques 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: $gcd(2^2 \cdot 3, 2^2 \cdot 3^2) = 2^2$
- 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: $lcm(2^2 \cdot 3^2, 2^3 \cdot 3) = 2^3 \cdot 3^2$

Theorem about LCM and GCD

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

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 very practical because prime factorization is computationally expensive!
- Much more efficient algorithm to compute gcd, called the Euclidian algorithm

Proof, cont.

- Show $i_k + j_k = \min(i_k, j_k) + \max(i_k, j_k)$
- Either (i) $i_k < j_k$ or (ii) $i_k \geq j_k$
- If (i), then $\min(i_k, j_k) = i_k$ and $\max(i_k, j_k) = j_k$
- Thus, $i_k + j_k = \min(i_k, j_k) + \max(i_k, j_k)$
- If (ii), then $\min(i_k, j_k) = j_k$ and $\max(i_k, j_k) = i_k$
- Hence $\min(i_k, j_k) + \max(i_k, j_k) = i_k + j_k$

Insight Behind Euclid’s Algorithm

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

- Theorem suggests following strategy to compute $\gcd(a, b)$:
  - Compute $r_1 = a \mod b$ ($\gcd(a, b) = \gcd(b, r_1)$)
  - Compute $r_2 = b \mod r_1$ ($\gcd(a, b) = \gcd(r_1, r_2)$)
  - Compute $r_3 = r_1 \mod r_2$ ($\gcd(a, b) = \gcd(r_2, r_3)$)
- Repeat until remainder becomes 0 ($\gcd(a, b) = \gcd(r_n, 0) = r_n$)
- The last non-zero remainder is the $\gcd$ of $a$ and $b$!

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, Euclidian algorithm gives us a way to compute these integers $s$ and $t$

Example

- Express $\gcd(252, 198)$ as a linear combination of 252 and 198
  - First apply Euclid’s algorithm (write $a = bq + r$ at each step):
    1. $252 = 1 \cdot 198 + 54$
    2. $198 = 3 \cdot 54 + 36$
    3. $54 = 1 \cdot 36 + 18$
    4. $36 = 2 \cdot 18 + 0$ \Rightarrow $\gcd$ is 18
  - Now, using (3), write 18 as $54 – 1 \cdot 36$
  - Using (2), write 18 as $54 – 1 \cdot (198 – 3 \cdot 54)$
  - Using (1), we have $54 = 252 – 1 \cdot 198$, thus:
    $$18 = (252 – 1 \cdot 198) – 1(198 – 3 \cdot (252 – 1 \cdot 198))$$

Example, cont.

- $18 = (252 – 1 \cdot 198) – 1(198 – 3 \cdot (252 – 1 \cdot 198))$
  - Now, let’s simplify this:
    $$18 = 252 – 1 \cdot 198 – 1 \cdot 198 + 3 \cdot 252 – 3 \cdot 198$$
  - Now, collect all 252 and 198 terms together:
    $$18 = 4 \cdot 252 – 5 \cdot 198$$
  - Trace steps of Euclid’s algorithm backwards to derive $s, t$:
    $$\gcd(a, b) = s \cdot a + t \cdot b$$
  - This is known as the extended Euclidian algorithm
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 \(\gcd(a, b) = 1\)
  - Multiply both sides by \(c\): \(c = csa + ctb\)
  - By earlier theorem, since \(a \mid bc\), \(a \mid ctb\)
  - Also, by earlier theorem, \(a \mid csa\)
  - Therefore, \(a \mid csa + ctb\), which implies \(a \mid c\) since \(c = csa + ctb\) 

Example

- **Lemma:** If \(a, b\) are relatively prime and \(a \mid bc\), then \(a \mid c\).
- **Suppose** \(15 \mid 16 \cdot x\)
- **Here** \(15\) and \(16\) are relatively prime
- **Thus**, previous theorem implies: \(15 \mid x\)

Question

- **Suppose** \(ca \equiv cb \pmod{m}\). Does this imply \(a \equiv b \pmod{m}\)?
- **Counterexample:** Consider \(14 \equiv 8 \pmod{6}\)
  - Thus, \(2 \cdot 7 \equiv 2 \cdot 4 \pmod{6}\)
  - But \(7 \not\equiv 4 \pmod{6}\)
  - Therefore, this implication does not hold in the general case!
- **However**, if \(c\) and \(m\) are relatively prime, it does hold

Another Useful Result

- **Theorem:** If \(ca \equiv cb \pmod{m}\) and \(\gcd(c, m) = 1\), then \(a \equiv b \pmod{m}\)
- **Proof:** Since \(ca \equiv cb \pmod{m}\), we have \(m \mid ca - cb\)
  - Rewriting, we get: \(m \mid c(a - b)\)
  - Since \(m, c\) are relatively prime, previous thm implies \(m \mid a - b\)
  - By definition of congruence, \(a \equiv b \pmod{m}\)

Examples

- If \(15x \equiv 15y \pmod{4}\), is \(x \equiv y \pmod{4}\)?
- If \(8x \equiv 8y \pmod{4}\), is \(x \equiv y \pmod{4}\)?
- **Counterexample:** \(8 \cdot 2 \equiv 8 \cdot 3 \pmod{4}\), but \(2 \not\equiv 3 \pmod{4}\)