BLG501E – Discrete Mathematics

2021 – 2022 Fall Term

Asst. Prof. Gökhan SEÇİNTİ

Outline

Noetherian Order (cont’d)

Ackerman Function

Number Theory

- Division
- Division Algorithm
- Modular Arithmetic
- Primes
- Greatest Common Divisors

Ackermann Function

$$A(m,n) = \begin{cases} \quad\quad if \quad\quad m = 0, A(m,n) = n+1 \\ else\,if \quad\quad n = 0, A(m,n) = A(m-1,1) \\ else\,if \;\; A(m,n) = A(m-1, A(m,n-1)) \end{cases}$$

Question:

A(3,1) = ?

Ackerman Function

Computable Equation Examples:

$$A(0, n) = n + 1$$
$$A(1, n) = n + 2$$
$$A(2, n) = 2n + 3$$
$$A(3, n) = 2^{n+3} - 3$$

…

Number Theory and Cryptography

Motivation

- *Number theory* is the part of mathematics devoted to the study of the integers and their properties.
- Key ideas in number theory include divisibility and the primality of integers.
- Representations of integers, including binary and hexadecimal representations, are part of number theory.
- Number theory has long been studied because of the beauty of its ideas, its accessibility, and its wealth of open questions.
- We’ll use many ideas developed in Chapter 1 about proof methods and proof strategy in our exploration of number theory.
- Mathematicians have long considered number theory to be pure mathematics, but it has important applications to computer science and cryptography studied in Sections 4.5 and 4.6.

Division

Definition: If a and b are integers with $a \neq 0$, then *a divides b* if there exists an integer c such that $b = ac$.

- When a divides b we say that a is a *factor* or *divisor* of b and that b is a multiple of a.
- The notation $a \mid b$ denotes that a divides b.
- If $a \mid b$, then b/a is an integer.
- If a does not divide b, we write $a \nmid b$.

Example: Determine whether $3 \mid 7$ and whether $3 \mid 12$.

Properties of Divisibility

Theorem 1: Let a, b, and c be integers, where $a \neq 0$.

i. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;

ii. If $a \mid b$, then $a \mid bc$ for all integers c;

iii. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof: (i) Suppose $a \mid b$ and $a \mid c$, then it follows that there are integers s and t with $b = as$ and $c = at$. Hence,

$$b + c = as + at = a(s + t). \quad \text{Hence, } a \mid (b + c)$$

◀

(Exercises 3 and 4 ask for proofs of parts (ii) and (iii).)

Corollary: If a, b, and c be integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

Can you show how it follows easily from from (ii) and (i) of Theorem 1?

Primes

Definition: A positive integer *p* greater than 1 is called *prime* if the only positive factors of *p* are 1 and *p*. A positive integer that is greater than 1 and is not prime is called *composite*.

$$p\ is\ a\ \mathbf{prime\ number} \Rightarrow p > 1 \land \neg[\exists q(q \in \{2,3,\ldots,p-1\} \land q|p)]$$

Example: The integer 7 is prime because its only positive factors are 1 and 7, but 9 is composite because it is divisible by 3.

The Fundamental Theorem of Arithmetic

Theorem: Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

$$a \in N^+,\ a = p_1^{k_1} p_2^{k_2} p_3^{k_3} \dots p_n^{k_n} \ \wedge \quad p_1 < p_2 < \cdots < p_n,\ p_i, k_i \in N$$

Examples:

- $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
- $641 = 641$
- $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$
- $1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

The Fundamental Theorem of Arithmetic

Theorem: If n is not a prime, at least one of its prime component cannot be greater than $\sqrt{n}$.

Proof:

$$n = a \cdot b \wedge \ a, b \in \boldsymbol{I}$$

(Contradiction) Assume both of the components are greater than $\sqrt{n}$.

$$a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$$

Division Algorithm

- When an integer is divided by a positive integer, there is a quotient and a remainder. This is traditionally called the "Division Algorithm," but is really a theorem.

Division Algorithm: If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$ (*proved in Section* 5.2).

- d is called the *divisor*.
- a is called the *dividend*.
- q is called the *quotient*.
- r is called the *remainder*.

Definitions of Functions
div and **mod**

$q = a$ **div** d
$r = a$ **mod** d

Examples:

- What are the quotient and remainder when 101 is divided by 11?
  Solution: The quotient when 101 is divided by 11 is $9 = 101$ **div** 11, and the remainder is $2 = 101$ **mod** 11.
- What are the quotient and remainder when -11 is divided by 3?
  Solution: The quotient when -11 is divided by 3 is $-4 = -11$ **div** 3, and the remainder is $1 = -11$ **mod** 3.

Greatest Common Divisor

Definition: Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and also $d \mid b$ is called the greatest common divisor of a and b. The greatest common divisor of a and b is denoted by gcd(a,b).

One can find greatest common divisors of small numbers by inspection.

Example:What is the greatest common divisor of 24 and 36?

Solution: gcd(24, 36) = 12

Example:What is the greatest common divisor of 17 and 22?

Solution: gcd(17,22) = 1

Greatest Common Divisor

Definition: $a, b \in I$

$$\boldsymbol{B} = \{x| \ \ x|a \wedge \ x|b\} \qquad \textit{forms a poset}$$

$$x' = \mathrm{gcd}(a, b) = \max(x|\, x \in \boldsymbol{B})$$

Greatest Common Divisor

Definition: The integers a and b are ***relatively prime*** if their greatest common divisor is 1.

Example: 17 and 22

Definition: The integers a_1, a_2, …, a_n are *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

Example: Determine whether the integers 10, 17 and 21 are pairwise relatively prime.

Solution: Because $\gcd(10,17) = 1$, $\gcd(10,21) = 1$, and $\gcd(17,21) = 1$, 10, 17, and 21 are pairwise relatively prime.

Example: Determine whether the integers 10, 19, and 24 are pairwise relatively prime.

Solution: Because $\gcd(10,24) = 2$, 10, 19, and 24 are not pairwise relatively prime.

Finding the Greatest Common Divisor Using Prime Factorizations

- Suppose the prime factorizations of *a* and *b* are:

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n} \ , \qquad b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n} \ ,$$

  where each exponent is a nonnegative integer, and where all primes occurring in either prime factorization are included in both. Then:

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \dots p_n^{\min(a_n,b_n)} \ .$$

- This formula is valid since the integer on the right (of the equals sign) divides both *a* and *b*. No larger integer can divide both *a* and *b*.

  Example: $120 = 2^3 \cdot 3 \cdot 5$ $\quad 500 = 2^2 \cdot 5^3$

  $\gcd(120,500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 3^0 \cdot 5^1 = 20$

- Finding the gcd of two positive integers using their prime factorizations is not efficient because there is no efficient algorithm for finding the prime factorization of a positive integer.

Least Common Multiple

Definition: The least common multiple of the positive integers *a* and *b* is the smallest positive integer that is divisible by both *a* and *b*. It is denoted by lcm(*a*,*b*).

- The least common multiple can also be computed from the prime factorizations.

$$\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$$

This number is divided by both *a* and *b* and no smaller number is divided by *a* and *b*.

Example: lcm($2^3 3^5 7^2$, $2^4 3^3$) = $2^{\max(3,4)}\, 3^{\max(5,3)}\, 7^{\max(2,0)} = 2^4\, 3^5\, 7^2$

- The greatest common divisor and the least common multiple of two integers are related by:

Theorem 5: Let a and b be positive integers. Then

$ab = \gcd(a,b) \cdot \text{lcm}(a,b)$

$(proof\ \ is\ Exercise\ 31)$

Euclidean Algorithm

- The Euclidian algorithm is an efficient method for computing the greatest common divisor of two integers. It is based on the idea that gcd(*a*,*b*) is equal to gcd(*a*,*c*) when $a > b$ and *c* is the remainder when a is divided by *b*.

Example: Find gcd$(91, 287)$:

- $287 = 91 \cdot 3 + 14$
- $91 = 14 \cdot 6 + 7$
- $14 = 7 \cdot 2 + 0$

Euclid
$(325$ B.C.E. – 265 B.C.E.$)$

gcd$(287, 91)$ = gcd$(91, 14)$ = gcd$(14, 7)$ = 7

continued →

Euclidean Algorithm

- The Euclidean algorithm expressed in pseudocode is:

```
procedure gcd(a, b: positive integers)
x := a
y := b
while  y ≠ 0
    r := x mod y
    x := y
    y := r
return x {gcd(a,b) is x}
```

- In Section 5.3, we'll see that the time complexity of the algorithm is $O(\log b)$, where $a > b$.

Euclidean Algorithm

Proof: $d = \gcd(a, b) \overset{?}{=} \gcd(b, r) = d', a = qb + r$

Part 1: Showing d also divides b and r

$$d|a \wedge d|b \Rightarrow d|a \wedge d|-qb \Rightarrow d|a - qb \Rightarrow d|r$$

Part 2: Showing d’ also divides a and b

$$d'|r \wedge d'|b \Rightarrow d'|r \wedge d'|qb \Rightarrow d'|r + qb \Rightarrow d'|a$$

Part 3: d and d’ are equal.

$$d = \gcd(a, b) = \mathrm{cd}(b, r) \leq \gcd(b, r) = d'$$
$$d' = \gcd(b, r) = \mathrm{cd}(a, b) \leq \gcd(a, b) = d$$

$$\left.\begin{matrix} d \leq d' \\ d' \leq d \end{matrix}\right\} d' = d$$

Congruence Relation

Definition: If a and b are integers and m is a positive integer, then a is *congruent to b modulo m* if m divides $a - b$.

- The notation $a \equiv b \pmod{m}$ says that a is congruent to b modulo m.
- We say that $a \equiv b \pmod{m}$ is a *congruence* and that m is its *modulus.*
- Two integers are congruent mod m if and only if they have the same remainder when divided by m.
- If a is not congruent to b modulo m, we write

$$a \not\equiv b \pmod{m}$$

Example: Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

Solution:

- $17 \equiv 5 \pmod{6}$ because 6 divides $17 - 5 = 12$.
- $24 \not\equiv 14 \pmod{6}$ since $24 - 14 = 10$ is not divisible by 6.

More on Congruences

Theorem 4: Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Proof:

- If $a \equiv b \pmod{m}$, then (by the definition of congruence) $m \mid a - b$. Hence, there is an integer k such that $a - b = km$ and equivalently $a = b + km$.
- Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$. Hence, $m \mid a - b$ and $a \equiv b \pmod{m}$.

◄

The Relationship between (mod m) and **mod** m Notations

- The use of "mod" in $a \equiv b \pmod{m}$ and a **mod** $m = b$ are different.
  - $a \equiv b \pmod{m}$ is a relation on the set of integers.
  - In a **mod** $m = b$, the notation **mod** denotes a function.
- The relationship between these notations is made clear in this theorem.
- **Theorem 3**: Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if a **mod** $m = b$ **mod** m. (*Proof in the exercises*)

Congruences of Sums and Products

Theorem 5: Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \text{ and } ac \equiv bd \pmod{m}$$

Proof:

- Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, by Theorem 4 there are integers s and t with $b = a + sm$ and $d = c + tm$.
- Therefore,
  - $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$ and
  - $b\,d = (a + sm)(c + tm) = ac + m(at + cs + stm)$.
- Hence, $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Example: Because $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, it follows from Theorem 5 that

$$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod{5}$$
$$77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod{5}$$

Algebraic Manipulation of Congruences

- Multiplying both sides of a valid congruence by an integer preserves validity.

  If $a \equiv b \pmod{m}$ holds then $c \cdot a \equiv c \cdot b \pmod{m}$, where c is any integer, holds by Theorem 5 with $d = c$.

- Adding an integer to both sides of a valid congruence preserves validity.

  If $a \equiv b \pmod{m}$ holds then $c + a \equiv c + b \pmod{m}$, where c is any integer, holds by Theorem 5 with $d = c$.

- Dividing a congruence by an integer does not always produce a valid congruence.

  Example: The congruence $14 \equiv 8 \pmod{6}$ holds. But dividing both sides by 2 does not produce a valid congruence since $14/2 = 7$ and $8/2 = 4$, but $7 \not\equiv 4 \pmod{6}$.

  See Section 4.3 for conditions when division is ok.

gcds as Linear Combinations

Étienne Bézout
(1730-1783)

Bézout's Theorem: If *a* and *b* are positive integers, then there exist integers *s* and *t* such that gcd(*a*,*b*) = *sa* + *tb*.

(*proof in exercises of Section* 5.2)

Definition: If *a* and *b* are positive integers, then integers *s* and *t* such that gcd(*a*,*b*) = *sa* + *tb* are called *Bézout coefficients* of *a* and *b.* The equation gcd(*a*,*b*) = *sa* + *tb* is called *Bézout's identity.*

- By Bézout's Theorem, the gcd of integers *a* and *b* can be expressed in the form *sa* + *tb* where *s* and *t* are integers. This is a *linear combination* with integer coefficients of *a* and *b*.
  - gcd(6,14) = $(-2)\cdot 6 + 1\cdot 14$

gcds as Linear Combinations

Étienne Bézout
(1730-1783)

Bézout's Theorem: If *a* and *b* are positive integers, then there exist integers *s* and *t* such that gcd(*a*,*b*) = *sa* + *tb*.

Extension: Smallest positive value of a linear combionation of two integers (a,b) is equal to gcd(a,b).

$$M = \{x | x = ma + nb \land m, n \in I\}, \qquad M = M^{-} \cup \{0\} \cup M^{+}$$
$$\gcd(a,b) = \min(M^{+})$$

Proof: next page ....

gcds as Linear Combinations

Étienne Bézout
(1730-1783)

$$a, b \in I, M = \{x | x = ma + nb \wedge m, n \in I\}, \qquad M = M^{-} \cup \{0\} \cup M^{+}$$

$$\gcd(a, b) = \min(M^{+})$$

Proof:

$$\gcd(a, b) = c \wedge \exists c_0 (c_0 \in M^{+} \wedge c_0 < c)$$
$$c_0 = m_0 a + n_0 b$$

$$c | a \wedge c | b \Rightarrow c | m_0 a + n_0 b \Rightarrow c | c_0$$

Contradiciton: c,c0 are positive and $c_0 < c$

That means any positive linear combination of a,b should be either equal or greater than gcd(a,b).

Finding gcds as Linear Combinations

Example: Express gcd(252,198) = 18 as a linear combination of 252 and 198.

Solution: First use the Euclidean algorithm to show gcd(252,198) = 18

i. $252 = 1 \cdot 198 + 54$
ii. $198 = 3 \cdot 54 + 36$
iii. $54 = 1 \cdot 36 + 18$
iv. $36 = 2 \cdot 18$

- Now working backwards, from iii and i above
  - $18 = 54 - 1 \cdot 36$
  - $36 = 198 - 3 \cdot 54$
- Substituting the 2nd equation into the 1st yields:
  - $18 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$
- Substituting $54 = 252 - 1 \cdot 198$ (from i)) yields:
  - $18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198$

- This method illustrated above is a two pass method. It first uses the Euclidian algorithm to find the gcd and then works backwards to express the gcd as a linear combination of the original two integers. A one pass method, called the *extended Euclidean algorithm*, is developed in the exercises.

Consequences of Bézout's Theorem

Lemma 2: If a, b, and c are positive integers such that gcd(a, b) = 1 and $a \mid bc$, then $a \mid c$.

Proof: Assume gcd(a, b) = 1 and $a \mid bc$

- Since gcd(a, b) = 1, by Bézout's Theorem there are integers s and t such that
  $sa + tb = 1$.
- Multiplying both sides of the equation by c, yields $sac + tbc = c$.
- From Theorem 1 of Section 4.1:
  $a \mid tbc$ (part ii) and a divides $sac + tbc$ since $a \mid sac$ and $a \mid tbc$ (part i)
- We conclude $a \mid c$, since $sac + tbc = c$.

Lemma 3: If p is prime and $p \mid a_1a_2\cdots a_n$, then $p \mid a_i$ for some i. ◄

(*proof uses mathematical induction; see Exercise 64 of Section 5.1*)

- Lemma 3 is crucial in the proof of the uniqueness of prime factorizations.

Consequences of Bézout's Theorem

Lemma 3: If p is prime and

$p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for some i.

Proof: $\exists i \; i \in \{1,2,\ldots,n\} \; p|a_i$

By induction:

$n = 1, p|a_1$ correct by initial definition

for n assume $p|a_1 a_2 \ldots a_n \Rightarrow \exists a_i \; p|a_i$

for $n+1, p| \; a_1 a_2 \ldots a_n a_{n+1} \Rightarrow p| \; A_n a_{n+1}$

either $\gcd(p, A_n) = 1$ or $\gcd(p, A_n) = p$

$\gcd(p, A_n) = 1$

$\gcd(A_n, p) = 1 \wedge p|A_n a_{n+1} \Rightarrow p|a_{n+1}$ *(Lemma2)*

Therefore

$\exists a_i, p|a_i$

$\gcd(p, A_n) = p$

$\gcd(A_n, p) = p \Rightarrow p|A_n$

By the assumption,

$\exists a_i, p|a_i$

Uniqueness of Prime Factorization

- We will prove that a prime factorization of a positive integer where the primes are in nondecreasing order is unique. (This part of the fundamental theorem of arithmetic. The other part, which asserts that every positive integer has a prime factorization into primes, will be proved in Section 5.2.)

  Proof: (*by contradiction*) Suppose that the positive integer n can be written as a product of primes in two distinct ways:

  $$n = p_1 p_2 \cdots p_s \text{ and } n = q_1 q_2 \cdots p_t.$$

  - Remove all common primes from the factorizations to get

    $$p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v}.$$

  - By Lemma 3, it follows that p_{i_1} divides q_{j_k}, for some *k*, contradicting the assumption that and $p_{i_1} q_{j_k}$ are distinct primes.

  - Hence, there can be at most one factorization of *n* into primes in nondecreasing order. ◀

Dividing Congruences by an Integer

- Dividing both sides of a valid congruence by an integer does not always produce a valid congruence (see Section 4.1).
- But dividing by an integer relatively prime to the modulus does produce a valid congruence:

Theorem 7: Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c,m) = 1$, then $a \equiv b \pmod{m}$.

Proof: Since $ac \equiv bc \pmod{m}$, $m \mid ac - bc = c(a - b)$ by Lemma 2 and the fact that $\gcd(c,m) = 1$, it follows that $m \mid a - b$. Hence, $a \equiv b \pmod{m}$.

◄

Additional Reads

Reads:

- Chap. 4 and 5, Discrete Math. and its applications, K.H. Rosen
- TBD