Chapter 4

The Number Theory and Cryptography

Chapter 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.

Chapter Summary

- Divisibility and Modular Arithmetic
- Integer Representations and Algorithms
- Primes and Greatest Common Divisors
- Solving Congruences
- Applications of Congruences
- Cryptography

4.1 Divisibility and Modular Arithmetic

Section Summary

- Division
- Division Algorithm
- Modular Arithmetic

Division

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

- 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 $\mathbf{3} \mid \mathbf{7}$ and whether $\mathbf{3} \mid \mathbf{12}$.

Properties of Divisibility

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

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

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

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

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

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 $\mathbf{0} \leq \boldsymbol{r} < \boldsymbol{d}$, such that $\boldsymbol{a} = \boldsymbol{dq} + \boldsymbol{r}$ (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.

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 not 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 $\boldsymbol{a = b + km}$.

Proof:

- If $a \equiv b \ (mod\ m)$, 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 $a \equiv b \ (mod\ m)$.

The Relationship between(mod m) and mod m Notations

- The use of “mod” in $\boldsymbol{a \equiv b}$ $(\boldsymbol{mod\ m})$ and $\boldsymbol{a\ mod\ m = b}$ are different.
  - $a \equiv b$ $(\mathbf{mod}\ m)$ is a relation on the set of integers.
  - In $a\ \mathbf{mod}\ m = b$, 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 $\boldsymbol{a \equiv b}$ $(\boldsymbol{mod\ m})$ if and only if $\boldsymbol{a\ mod\ m = b\ mod\ m}$. (Proof in the exercises)

Congruences of Sums and Products

- **Theorem 5:** Let m be a positive integer. If $\boldsymbol{a \equiv b \ (mod\ m)}$ and $\boldsymbol{c \equiv d \ (mod\ m)}$, then $\boldsymbol{a + c \equiv b + d \ (mod\ m)}$ and $\boldsymbol{ac \equiv bd \ (mod\ m)}$.

Proof:

- Because $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$, 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, $a + c \equiv b + d \ (mod\ m)$ and $ac \equiv bd \ (mod\ m)$.

Example: 7≡ 2$(\boldsymbol{mod}\ \mathbf{5})$ and $\mathbf{11} \equiv \mathbf{1}\ (\boldsymbol{mod}\ \mathbf{5})$, it follows from Theorem 5 that

- $18 = 7 + 11 \equiv 2 + 1 = 3\ (mod\ 5)$
- $77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2\ (mod\ 5)$

Algebraic Manipulation of Congruences

- Multiplying both sides of a valid congruence by an integer preserves validity.
  - If $a \equiv b \ (mod\ m)$ holds then $c \cdot a \equiv c \cdot b \ (mod\ m)$, 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 $a \equiv b \ (mod\ m)$ holds $then\ c + a \equiv c + b \ (mod\ m)$, 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 $\mathbf{14 \equiv 8 \ (\mathit{mod}\ 6)}$ holds. But dividing both sides by 2 does not produce a valid congruence since 14/2 = 7 and 8/2 = 4, but $\mathbf{7 \not\equiv 4 \ (\mathit{mod}\ 6)}$.

See Section 4.3 for conditions when division is ok.

Computing the mod m Function of Products and Sums

- We use the following corollary to Theorem 5 to compute the remainder of the product or sum of two integers when divided by m from the remainders when each is divided by m.

- Corollary:
  - Let m be a positive integer and let a and b be integers.
  - Then, $(a + b)\ (mod\ m) = ((a\ mod\ m) + (b\ mod\ m))\ mod\ m$
  - And, $ab\ mod\ m = ((a\ mod\ m)\ (b\ mod\ m))\ mod\ m.\ (proof\ \ in\ text)$

Arithmetic Modulo m1

Definitions: Let Z_m be the set of nonnegative integers less than m: $\{0,1, \ldots., m-1\}$

- The operation +m is defined as $a +_m b = (a + b)\ mod\ m$. This is addition modulo m.
- The operation ·m is defined as $a \cdot_m b = (a \cdot b)\ mod\ m$. This is multiplication modulo m.
- Using these operations is said to be doing arithmetic modulo m.

Example: Find $\mathbf{7 +_{11} 9}$ $\boldsymbol{and}$ $\mathbf{7 \cdot_{11} 9}$.

Solution: Using the definitions above:

- $7 +_{11} 9 = (7 + 9)\ mod\ 11 = 16\ mod\ 11 = 5$
- $7 \cdot_{11} 9 = (7 \cdot 9)\ mod\ 11 = 63\ mod\ 11 = 8$

Arithmetic Modulo m2

The operations $+_m$ and $\cdot_m$ satisfy many of the same properties as ordinary addition and multiplication.

- **Closure:**

  If a and b belong to Z_m , then $a +_m b$ and $a \cdot_m b$ belong to Z_m .

- **Associativity:**

  If a, b, and c belong to Z_m , then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.

- **Commutativity:**

  If a and b belong to Z_m , then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.

- **Identity elements:**

  The elements 0 and 1 are identity elements for addition and multiplication modulo m, respectively. If a belongs to Z_m , then $a +_m 0 = a$ and $a \cdot_m 1 = a$.

Arithmetic Modulo m₃

- **Additive inverses:**

  If $a \neq 0$ belongs to Z_m, then $m - a$ is the additive inverse of a modulo m and 0 is its own additive inverse.

  $$a +_m (m - a) = 0 \; and \; 0 +_m 0 = 0$$

- **Distributivity:**

  If a, b, and c belong to Z_m, then $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.

Exercises 42-44 ask for proofs of these properties.

- Multiplicatative inverses have not been included since they do not always exist. For example, there is no multiplicative inverse of 2 modulo 6.

Homework:

SE: P. 244 12,30,32

EE: P. 258 16,36,38

4.3 Primes and Greatest Common Divisors

Section Summary

- Prime Numbers and their Properties
- Conjectures and Open Problems About Primes
- Greatest Common Divisors and Least Common Multiples i
- The Euclidian Algorithm
- gcds as Linear Combinations

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.

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.

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 Sieve of Erastosthenes[1]

- The Sieve of Erastosthenes can be used to find all primes not exceeding a specified positive integer. For example, begin with the list of integers between 1 and 100.

a. Delete all the integers, other than 2, divisible by 2.

b. Delete all the integers, other than 3, divisible by 3.

c. Next, delete all the integers, other than 5, divisible by 5.

d. Next, delete all the integers, other than 7, divisible by 7.

e. Since all the remaining integers are not divisible by any of the previous integers, other than 1, the primes are:

{2,3,5,7,11,15,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97}

Erastothenes
(276-194 B.C.)

The Sieve of Erastosthenes$_2$

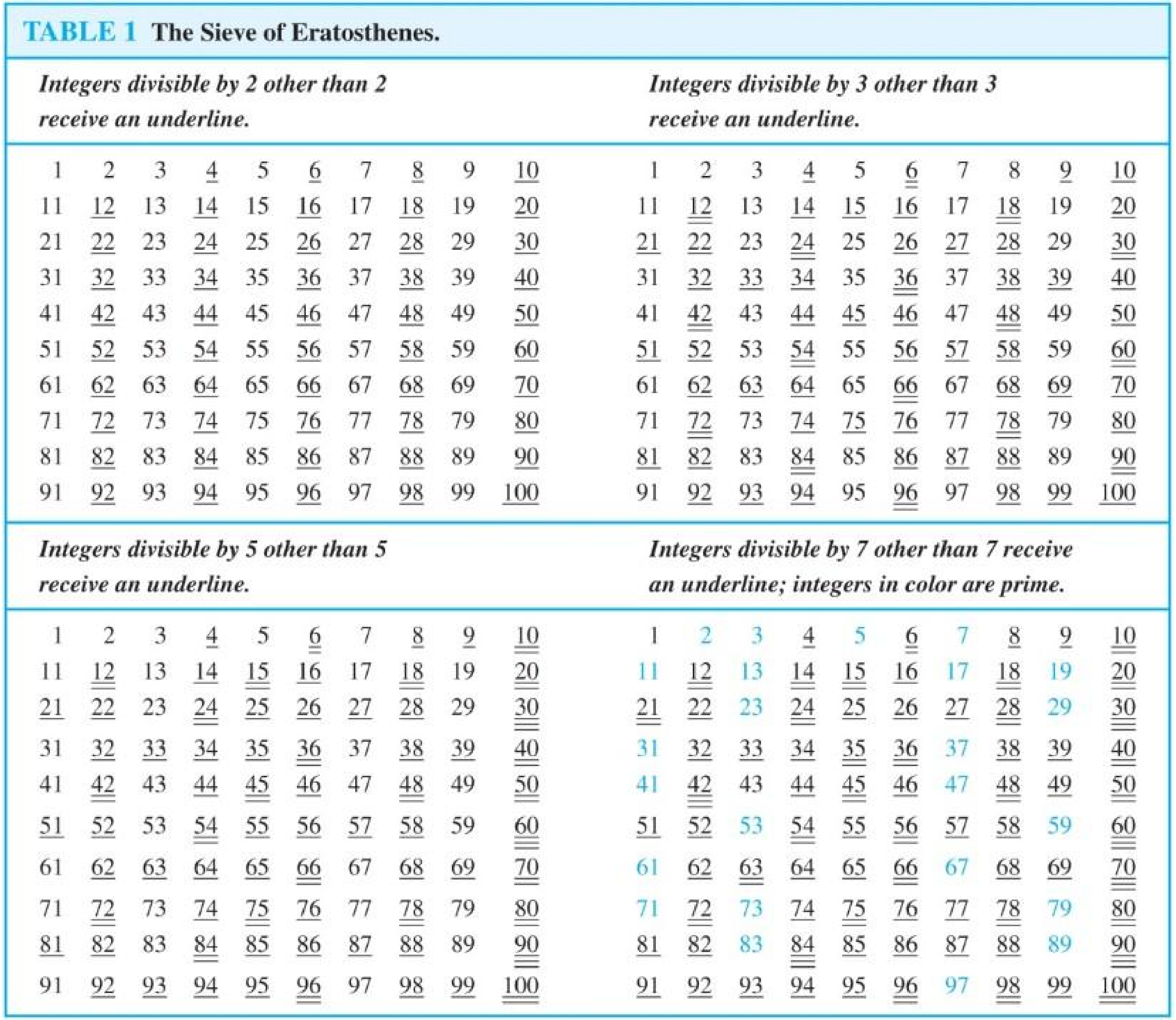


TABLE 1 The Sieve of Eratosthenes.

Integers divisible by 2 other than 2 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 3 other than 3 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 5 other than 5 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 7 other than 7 receive an underline; integers in color are prime.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

If an integer n is a composite integer, then it has a prime divisor less than or equal to $\sqrt{n}$.

To see this, note that if $n = ab$, then $a \le \sqrt{n}$ or $b \le \sqrt{n}$.

Trial division, a very inefficient method of determining if a number n is prime, is to try every integer $i \le \sqrt{n}$ and see if n is divisible by i.

Infinitude of Primes

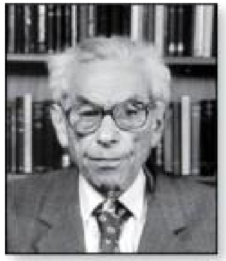
- **Theorem:** There are infinitely many primes. (Euclid)

Euclid
(325 B.C.E. – 265 B.C.E.)

Proof: Assume finitely many primes: $\boldsymbol{p_1, p_2, p_3 \ldots, p_n}$

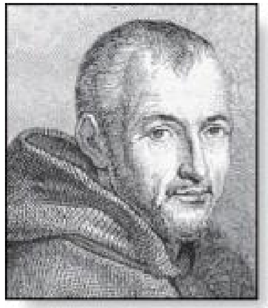
- Let $q = p_1 p_2 \ldots p_n + 1$
- Either q is prime or by the fundamental theorem of arithmetic it is a product of primes.
  - But none of the primes p_j divides q since if $p_j \mid q$, then p_j divides $q - p_1 p_2 \cdots p_n = 1$.
  - Hence, there is a prime not on the list $p_1, p_2, \ldots.., p_n$. It is either q, or if q is composite, it is a prime factor of q. This contradicts the assumption that $p_1, p_2, \ldots, p_n$ are all the primes.
- Consequently, there are infinitely many primes.

This proof was given by Euclid The Elements. The proof is considered to be one of the most beautiful in all mathematics. It is the first proof in The Book, inspired by the famous mathematician Paul Erdős' imagined collection of perfect proofs maintained by God.



Paul Erdős
(1913-1996)

Mersenne primes



Marin Mersenne
(1588-1648)

- **Definition: Prime numbers of the form $2^p - 1$, where p is prime, are called Mersenne primes.**
  - $2^2 - 1 = 3,\ 2^3 - 1 = 7,\ 2^5 - 1 = 37\ , and\ 2^7 - 1 = 127$ are Mersenne primes.
  - $2^{11} - 1 = 2047$ is not a Mersenne prime since 2047 = 23·89.
  - There is an efficient test for determining if $2^p - 1$ is prime.
  - The largest known prime numbers are Mersenne primes.
  - As of early 2018, 50 Mersenne primes were known, the largest is $2^{77,232,917} – 1$, which has nearly 23 million decimal digits.
  - The Great Internet Mersenne Prime Search (GIMPS) is a distributed computing project to search for new Mersenne Primes.

http://www.mersenne.org/

Distribution of Primes

- Mathematicians have been interested in the distribution of prime numbers among the positive integers. In the nineteenth century, the prime number theorem was proved which gives an asymptotic estimate for the number of primes not exceeding x.

- Prime Number Theorem: The ratio of the number of primes not exceeding x and $x/ln\, x$ approaches 1 as x grows without bound. ($ln\, x$ is the natural logarithm of x)
    - The theorem tells us that the number of primes not exceeding x, can be approximated by $x/\ln x$.
    - The odds that a randomly selected positive integer less than n is prime are approximately $(n/\ln n)/n \; = \; 1/\ln n$.

Generating Primes

The problem of generating large primes is of both theoretical and practical interest.

We will see (in Section 4.6) that finding large primes with hundreds of digits is important in cryptography.

So far, no useful closed formula that always produces primes has been found. There is no simple function *f*(*n*) such that *f*(*n*) is prime for all positive integers *n*.

But $f(n) = n^2 - n + 41$ is prime for all integers $1, 2, \ldots, 40$. Because of this, we might conjecture that *f*(*n*) is prime for all positive integers *n*. But $f(41) = 41^2$ is not prime.

More generally, there is no polynomial with integer coefficients such that $f(n)$ is prime for all positive integers *n*. (See supplementary Exercise 23.)

Fortunately, we can generate large integers which are almost certainly primes. See Chapter 7.

Conjectures about Primes

Even though primes have been studied extensively for centuries, many conjectures about them are unresolved, including:

- ***Goldbach's Conjecture*: Every even integer n, $n > 2$, is the sum of two primes. It has been verified by computer for all positive even integers up to $4 \cdot 10^{18}$. The conjecture is believed to be true by most mathematicians.**
- **There are infinitely many primes of the form $n^2 + 1$, where n is a positive integer. But it has been shown that there are infinitely many positive integer n such that $n^2 + 1$ is a primes or the product of at most two primes.**
- ***The Twin Prime Conjecture*: The twin prime conjecture is that there are infinitely many pairs of twin primes. Twin primes are pairs of primes that differ by 2. Examples are 3 and 5, 5 and 7, 11 and 13, etc. The current world's record for twin primes (as of early 2018) consists of numbers $2{,}996{,}863{,}034{,}895 \cdot 2^{1{,}290{,}000} \pm 1$, which have 388,342 decimal digits.**

Greatest Common Divisor[1]

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

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

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

Solution: $\boldsymbol{gcd(24,\ 36)\ =\ 12}$

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

Solution: $\boldsymbol{gcd(17, 22)\ =\ 1}$

Greatest Common Divisor2

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

Example: 17 and 22

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

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

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

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

Solution: Because $\boldsymbol{gcd(10,24) = 2}$, $\boldsymbol{10,\ 19,\ and\ 24}$ 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:

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

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

Finding the $\boldsymbol{gcd}$ 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 $\boldsymbol{lcm(a,b)}$.

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

$$\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \ldots p_n^{\max(a_n,bn)},$$

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

Example: $lcm(233572,\ 2433) \ = \ 2^{\max(3,4)}\, 3^{\max(5,3)}\, 7^{\max(2,0)} \ = \ 2^4\, 3^5\, 7^2$

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

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

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

Euclidean Algorithm[1]

Euclid
(325 B.C.E. – 265 B.C.E.)

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 $gcd(\mathrm{b}, \mathrm{r})$ when $a > b$ and c is the remainder when a is divided by b.

Example: Find $\boldsymbol{gcd(91,\ 287)}$:

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

Stopping condition

$$\boldsymbol{gcd(287,\ 91) = gcd(91,\ 14) = gcd(14,\ 7) = 7}$$

Correctness of Euclidean Algorithm[1]

◆ **Lemma 1: Let $a = bq + r$, where a, b, q, and r are integers. Then $gcd(a, b) = gcd(b, r)$.**

Proof:

- Suppose that d divides both a and b. Then d also divides $a - bq = r$ (by **Theorem 1** of **Section 4.1**). Hence, any common divisor of a and b must also be any common divisor of b and r.
- Suppose that d divides both b and r. Then d also divides $bq + r = a$.
- Hence, any common divisor of a and b must also be a common divisor of b and r.
- Therefore, $\text{gcd}(a, b) = \text{gcd}(b, r)$.

Correctness of Euclidean Algorithm2

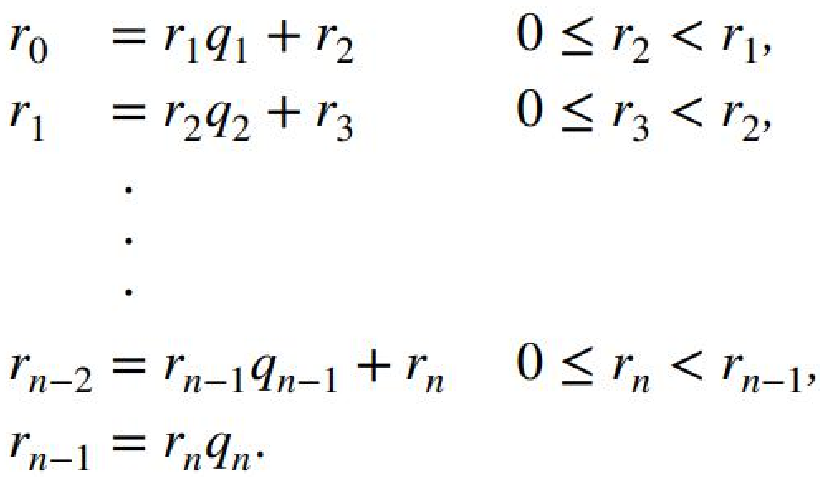
Suppose that a and b are positive

integers with $a \geq b$.

Let r_0= a and r_1 = b.

Successive applications of the division

algorithm yields:



$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 && 0 \leq r_2 < r_1, \\
r_1 &= r_2 q_2 + r_3 && 0 \leq r_3 < r_2, \\
&\cdot \\
&\cdot \\
&\cdot \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n && 0 \leq r_n < r_{n-1}, \\
r_{n-1} &= r_n q_n.
\end{aligned}$$

Eventually, a remainder of zero occurs in the sequence of terms: a $= r_0 > r_1 > r_2 > \cdots \geq 0$. The sequence can't contain more than a terms.

By Lemma 1

$\gcd(a, b) = \gcd(r_0, r_1) = \cdot \cdot \cdot = \gcd(r_{n-1}, rn) = \gcd(r_n, 0) = r_n$.

Hence the greatest common divisor is the last nonzero remainder in the sequence of divisions.

Euclidean Algorithm$_2$

The Euclidean algorithm expressed in pseudocode is:

```
procedure $gcd(a, b$: positive integers)
$x := a$
$y := b$
while  $y \neq 0$
        $r := x$ 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.

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 $\boldsymbol{gcd(a,b) = sa + tb}$.

  (proof in exercises of Section 5.2)

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

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

Find Bézout coefficients

Example: Express $\boldsymbol{gcd}(\mathbf{252},\mathbf{198}) = \mathbf{18}$ as a linear combination of 252 and 198.

Solution: First use the Euclidean algorithm to show $\boldsymbol{gcd}(\mathbf{252},\mathbf{198}) = \mathbf{18}$.

i. 252 = 1·198 + 54. ii. 198 = 3 ·54 + 36

iii. 54 = 1 ·36 + 18 iv. 36 = 2 ·18

- Now working backwards, from (iii) and (ii) above
  - 18 = 54 − 1 ·36
  - 36 = 198 − 3 ·54
- Substituting the 2nd equation into the 1st yields:
  - 18 = 54 − 1 ·(198 − 3 ·54)= 4 ·54 − 1 ·198
- Substituting 54 = 252 − 1 ·198 (from i)) yields:
  - 18 = 4 ·(252 − 1 ·198) − 1 ·198 = 4 ·252 − 5 ·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 $\boldsymbol{gcd(a,\ b)\ =\ 1}$ and $\boldsymbol{a \mid bc}$, then $\boldsymbol{a \mid c}$.

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

- 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 $a|tbc$ (part i)
- We conclude $a \mid c$, since $sac\ +\ tbc\ =\ c$.

- Lemma 3: If p is prime and $\boldsymbol{p \mid a_1a_2 \cdots a_n}$, then $\boldsymbol{p \mid a_i}$ 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.

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:

$$n = p_1p_2 \cdots p_s \text{ and } n = q_1q_2 \cdots p_t.$$

- Remove all common primes from the factorizations to get $p_{i1}p_{i2} \cdots p_{iu} = q_{j1}q_{j2} \cdots q_{jv}$
- By Lemma 3, it follows that p_{i1} divides q_{jk} for some k, contradicting the assumption that and 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 $\boldsymbol{ac \equiv bc \ (mod\ m)}$ and $\boldsymbol{gcd(c, m) = 1}$, then $\boldsymbol{a \equiv b \ (mod\ m)}$.

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

Homework:

SE: P. 273 32(d,f),34,40(d,g),50

EE: P. 289 32(d,f),34,40(d,g),50