# Primes and Greatest Common Divisors

Section 4.3

# Section Summary 3

Prime Numbers and their Properties

Greatest Common Divisors and Least Common Multiples

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.

The existence was proved by induction in Chapter 5. The uniqueness will be proved in this section,

**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 1,2,...,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:

{2,3,5,7,11,15,1719,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89, 97}

In applying this metnod to find the primes in {1,2,...,m}, stop after reaching the largest prime not exceeding the square root of m.

You can stop after deleting the multiples of the largest prime not exceeding $\sqrt{m}$ because

# The Sieve of Erastosthenes

Finding all primes in the set {1,2,...,100}

**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 $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

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

# Infinitude of Primes

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

**Proof**: Assume finitely many primes: $p_1, p_2, \ldots, p_n$

- Let $q = p_1 p_2 \cdots p_n + 1$
- Either $q$ is prime or is a product of primes.
  - But none of the primes $p_j$ divides $q$ since if $p_j \mid q$, then $p_j$ divides $q - p_1 p_2 \cdots p_n = 1$ but the primes do not divide 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.

Note: There is no explicit formula that gives the n-th prime in terms of n.

# Greatest Common Divisor 1

**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

divisors of 24 are 1,2,4,6,8,12,24
divisors of 36 are 1,2,3,4,6,9,12,18, 36

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

**Solution**: gcd(17,22) = 1

divisors of 17 are 1,17
divisors of 22 are 1,2,11,22

# Greatest Common Divisor 2

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

**Example**: 17 and 22

**Definition**: The integers $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$. We need only consider the pairs where i < j because gcd(p,q)=gcd(q,p)

**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:

This is not the usual prime factorization. Exponents can be zero.

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

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

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

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**: $120 = 2^3 \cdot 3^1 \cdot 5^1$ $500 = 2^2 \cdot 5^3 = 2^2 \cdot 3^0 \cdot 5^3$

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

While this works for small integers,

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.

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

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

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

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

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

# Euclidean Algorithm[1]

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(b,r) when $a > b$ and r is the remainder when a is divided by *b*.

gcd(a,a)=a and gcd(a,b) =gcd(b,a) if the given numbers are different.

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

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

Divide 287 by 91

Divide 91 by 14

Divide 14 by 7

Stopping condition

Start by dividing the larger number by the smaller. when going from one step to the next, the previous divisor becomes the new dividend and the previous remainder becomes the new divisor

Stop when the remainder is zero. the gcd is the previous remainder.

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**: We have a = bq + r and r = a - bq

- 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 b and r must also be a common divisor of a and b.

  The set of common divisors of a and b is the same as the set of common divisors of b and r.
- Therefore, $\gcd(a,b) = \gcd(b,r)$.

# Correctness of Euclidean Algorithm 2

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:

$$r_0 = r_1 q_1 + r_2 \qquad 0 \leq r_2 < r_1,$$
$$r_1 = r_2 q_2 + r_3 \qquad 0 \leq r_3 < r_2,$$
$$\vdots$$
$$r_{n-2} = r_{n-1} q_{n-1} + r_n \qquad 0 \leq r_n < r_{n-1},$$
$$r_{n-1} = r_n q_n + 0$$

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

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

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

# gcds as Linear Combinations

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

**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 $b$.

- $\gcd(6,14) = (-2)\cdot 6 + 1\cdot 14 = 2$

**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 ii
  - $18 = 54 - 1 \cdot 36$
  - $36 = 198 - 3 \cdot 54$
- 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.

# 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:
  $a \mid tbc$ then $a$ divides $sac + tbc$ since $a \mid sac$ and $a \mid tbc$
- We conclude $a \mid c$, since $sac + tbc = c$.

**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 uses mathematical induction*)

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 is part of the fundamental theorem of arithmetic. The other part, which asserts that every positive integer has a prime factorization into primes, was proved in section 5.2.

***Proof (of the uniqueness of the prime factorization of a positive integer):*** We will use a proof by contradiction. Suppose that the positive integer $n$ can be written as the product of primes in two different ways, say, $n = p_1 p_2 \cdots p_s$ and $n = q_1 q_2 \cdots q_t$, where each $p_i$ and $q_j$ is prime such that $p_1 \leq p_2 \leq \cdots \leq p_s$ and $q_1 \leq q_2 \leq \cdots \leq q_t$.

When we remove all common primes from the two factorizations, we have

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

where no prime occurs on both sides of this equation and $u$ and $v$ are positive integers. By Lemma 3 it follows that $p_{i_1}$ divides $q_{j_k}$ for some $k$. Because no prime divides another prime, this is impossible. Consequently, 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**: 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, $a \equiv b \pmod{m}$.