


# Discrete Math

## Ch4: Numbers

### Tutorial 6

**EXAMPLE 1** Determine whether  $3 \mid 7$  and whether  $3 \mid 12$ .

*Solution:* We see that  $3 \nmid 7$ , because  $7/3$  is not an integer. On the other hand,  $3 \mid 12$  because  $12/3 = 4$ . 

Let  $a$ ,  $b$ , and  $c$  be integers, where  $a \neq 0$ . Then

- (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  $a \mid c$ .

**THE DIVISION ALGORITHM** Let  $a$  be an integer and  $d$  a positive integer. Then there are unique integers  $q$  and  $r$ , with  $0 \leq r < d$ , such that  $a = dq + r$ .

In the equality given in the division algorithm,  $d$  is called the *divisor*,  $a$  is called the *dividend*,  $q$  is called the *quotient*, and  $r$  is called the *remainder*. This notation is used to express the quotient and remainder:


$$q = a \text{ div } d, \quad r = a \text{ mod } d.$$

- The remainder is always less than the divisor. If the remainder is greater than the divisor, it means that the division is incomplete.

What are the quotient and remainder when 101 is divided by 11?

*Solution:* We have

$$101 = 11 \cdot 9 + 2.$$

Hence, the quotient when 101 is divided by 11 is  $9 = 101 \text{ div } 11$ , and the remainder is  $2 = 101 \text{ mod } 11$ . 

---

What are the quotient and remainder when  $-11$  is divided by 3?


*Solution:* We have

$$-11 = 3(-4) + 1.$$

Hence, the quotient when  $-11$  is divided by 3 is  $-4 = -11 \text{ div } 3$ , and the remainder is  $1 = -11 \text{ mod } 3$ .

Note that the remainder cannot be negative. Consequently, the remainder is *not*  $-2$ , even though

$$-11 = 3(-3) - 2,$$

because  $r = -2$  does not satisfy  $0 \leq r < 3$ . 

**13.** What are the quotient and remainder when

**a)** 19 is divided by 7?

**b)** 789 is divided by 23?

**c)** 1001 is divided by 13?

**d)** 0 is divided by 19?

**Answer:**

a) quotient = 2, remainder = 5

b) quotient = 34, remainder = 7

c) quotient = 77, remainder = 0

d) quotient = 0, remainder = 0

**28.** Find  $a \text{ div } m$  and  $a \text{ mod } m$  when

**a)**  $a = -111$ ,  $m = 99$ .

**b)**  $a = -9999$ ,  $m = 101$ .

**(a)**

For  $a = -111$  and  $m = 99$ .

Rewrite  $-111$  as:

$$-111 = 99(-2) + 87$$

Here, the quotient when  $-111$  is divided by  $99$  is  $-2 = -111 \text{ div } 99$ , and the remainder is  $87 = -111 \text{ mod } 99$ .

Therefore,  $a \text{ div } m = \boxed{-2}$  and  $a \text{ mod } m = \boxed{87}$ .

B, Assignment

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

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

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

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

and that

$$77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod{5}.$$



## Arithmetic Modulo $m$

$$a +_m b = (a + b) \bmod m,$$

$$a \cdot_m b = (a \cdot b) \bmod m,$$

Use the definition of addition and multiplication in  $\mathbf{Z}_m$  to find  $7 +_{11} 9$  and  $7 \cdot_{11} 9$ .

*Solution:* Using the definition of addition modulo 11, we find that


$$7 +_{11} 9 = (7 + 9) \bmod 11 = 16 \bmod 11 = 5,$$

and

$$7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8.$$

## Primes

An 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*.

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

**THE FUNDAMENTAL THEOREM OF ARITHMETIC** Every 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 prime factorizations of 100, 641, 999, and 1024 are given by

$$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2,$$

$$641 = 641,$$

$$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37,$$

$$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}.$$

**3.** Find the prime factorization of each of these integers.

**a)** 88

**b)** 126

**c)** 729

**d)** 1001

**a)**  $88 = 2^3 \cdot 11$


**b)**  $126 = 2 \cdot 63 = 2 \cdot 3 \cdot 21 = 2 \cdot 3 \cdot 3 \cdot 7 = 2 \cdot 3^2 \cdot 7$

## Greatest Common Divisors

Let  $a$  and  $b$  be integers, not both zero. The largest integer  $d$  such that  $d \mid a$  and  $d \mid b$  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 way to find the greatest common divisor of two integers is to find all the positive common divisors of both integers and then take the largest divisor

What is the greatest common divisor of 24 and 36?

*Solution:* The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6, and 12. Hence,  $\gcd(24, 36) = 12$ . 

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

What is the greatest common divisor of 17 and 22?

*Solution:* The integers 17 and 22 have no positive common divisors other than 1, so that  $\gcd(17, 22) = 1$ . 

17 and 22 are **relatively prime**, because  $\gcd(17, 22) = 1$

## Greatest Common Divisors using prime factorization

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

Because the prime factorizations of 120 and 500 are  $120 = 2^3 \cdot 3 \cdot 5$  and  $500 = 2^2 \cdot 5^3$ , the greatest common divisor is

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



## Least Common Multiple

Prime factorizations can also be used to find the **least common multiple** of two integers.

The *least common multiple* of the positive integers  $a$  and  $b$  is the smallest positive integer that is divisible by both  $a$  and  $b$ . The least common multiple of  $a$  and  $b$  is denoted by  $\text{lcm}(a, b)$ .

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

What is the least common multiple of  $2^3 3^5 7^2$  and  $2^4 3^3$ ?

*Solution:* We have

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