

1. Formal Definition of “divides”

Given two integers $d > 0$ and a .

We say d **divides** a if and only there is an integer q (called the quotient) such that

$$a = qd.$$

We also say, a is a **multiple** of d .

3. Zero

In the statement d divides a , we do not allow $d = 0$.

On the other hand, there is no problem taking $a = 0$.

Indeed, any positive integer d divides 0 with quotient 0.

5. Letters

Mathematicians commonly use letters based on English spelling.

The formula for the area of a circle $A = \pi R^2$ uses A for area and R for radius.

We often write f for function or p for prime.

Our definition of “quotient and remainder” follows this convention by using d for divisor, q for quotient, and r for remainder.

7. Equivalent statements

The following 5 statements are equivalent:

- (1) d divides a
- (2) a is a multiple of d
- (3) $a = qd$ for some integer q
- (4) the remainder when you divide a by d is 0
- (5) $a \bmod d = 0$

9. Questions

What are the primes good for?

How many primes are there?

How far apart can primes be?

Is there some simple way to tell if a number is prime?

These questions (and more) will be answered in this module.

2. Some examples

- (1) 10 divides 90, with quotient 9
- (2) 7 divides 35, with quotient 5
- (3) 23 divides 2047, with quotient 89

4. Quotient and Remainder

In general, we can always divide any integer a by $d > 0$, getting a **quotient** q and **remainder** r :

$$a = qd + r,$$

where the remainder is restricted to the interval $0 \leq r \leq d - 1$.

6. Some examples

- (1) $a = 87, d = 20$: $87 = 4 \times 20 + 7$
- (2) $a = 2^6 = 64, d = 7$: $64 = 9 \times 7 + 1$
- (3) $a = 366, d = 7$: $366 = 52 \times 7 + 2$

8. Primes and Composites

A positive integer greater than 1 is **prime** if its only divisors are 1 and itself.

The List of Primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, etc

But not $4 = 2 \times 2$, $6 = 2 \times 3$, etc.

A positive integer n greater than 1 which is not prime is called a **composite** number.

The number 1 is called a **unit**. It is neither prime nor composite.

10. Factoring Composites

Every positive composite integer n splits into a product

$$n = a \cdot b$$

where both a and b are ≥ 2 .

11. Factoring $n = 30$

There are three different ways to factor $n = 30$ into two pieces:

- (1) $30 = 2 \times 15$
- (2) $30 = 3 \times 10$
- (3) $30 = 5 \times 6$

12. Factoring 30 into primes

If we keep factoring until we get primes:

- (1) $30 = 2 \times 15 = 2 \times 3 \times 5$
- (2) $30 = 3 \times 10 = 3 \times 2 \times 5$
- (3) $30 = 5 \times 6 = 5 \times 2 \times 3$

In each case we get the same three primes—2, 3, 5—not counting order.

13. The Fundamental Theorem of Arithmetic

Every integer $n > 1$ is either prime, or a product of a unique set of primes.

We will prove the Fundamental Theorem in Section 1 of this module.

14. A 19th Century Puzzler

In the 19th Century a group of mathematicians began to study algebraic structures similar to the integers. One of the pioneers of this group was Ernst Kummer. (Google Search his name to find more information.) Naively they assumed, at first, that numbers in these new systems would factor uniquely into primes, like the integers. They were wrong.

15. Greatest Common Divisor

The **greatest common divisor** of a and b (not both 0) is the largest number that divides both a and b .

We abbreviate “greatest common divisor” as GCD.

Examples:

- (1) $\text{GCD}(30, 18) = 6$
- (2) $\text{GCD}(25, 35) = 5$
- (3) $\text{GCD}(1001, 154) = 77$

16. Relatively Prime Integer

When $\text{GCD}(a, b) = 1$, we say that a and b are **relatively prime**.

For example, 15 and 28 are relatively prime, even though neither number is a prime itself.

The point is that $15 = 3 \times 5$ and $28 = 2 \times 2 \times 7$ have no factors in common.

Recall that in order to solve the pails of water problem $\text{POW}(a, b)$, the numbers a and b must be relatively prime.

17. Least Common Multiple

The **least common multiple** of two nonzero integers a and b is the smallest positive number that is divisible by both a and b .

We abbreviate “least common multiple” as LCM.

Examples:

- (1) $\text{LCM}(15, 35) = 105$
- (2) $\text{LCM}(100, 210) = 2100$
- (3) $\text{GCD}(9, 49) = 441$

18. Common Denominators

The common denominator you use when adding two fractions

$$\frac{a}{b} + \frac{c}{d}$$

is the least common multiple of the two denominators b and d .