

Greatest Common Divisor

Definition 1. Suppose $d|a$ and $d|b$. Then d is called a **common divisor** of a and b .

Example: Common divisors of 14 and 18 are $\pm 1, \pm 2$.

Definition 2. If a and b are not both 0, then the largest positive common divisor g of a and b is called the **greatest common divisor** of a and b .

Notation: Write $d = \gcd(a, b)$ or just $g = (a, b)$.

Example: $\gcd(14, 18) = 2$.

Notation: When $\gcd(a, b) = 1$ we say that a and b are **relatively prime** or that a is **relatively prime** to b . Another way of saying this is to assert that a and b share no common factors.

Example. 144 and 35 are relatively prime, while 21 and 35 are not.

Fact: If p is a prime,

$$\gcd(p, a) = \begin{cases} 1 & \text{if } p \nmid a \\ p & \text{if } p|a. \end{cases}$$

Fact: If $a \neq 0$ and $b = qa + r$, then the common divisors of a and b are the same as the common divisors of a and r . In particular,

$$(a, b) = (r, a).$$

Example. Compute $(100, 68)$.

Solution:

$$\begin{aligned} (68, 100) &= (32, 100) & 100 &= 1 \cdot 68 + 32 \\ (32, 68) &= (4, 32) & 68 &= 2 \cdot 32 + 4 \\ (4, 32) &= 4 & 4 &\text{ divides } 32 \end{aligned}$$

Example. Compute $(12471, 149751)$.