

② Elementary number theory

Def. 2.1 Let a and b be integers with $b \neq 0$. We say that b divides a , or that a is divisible by b , if there is an integer c such that

$$a = c \cdot b.$$

We write $b|a$ to indicate that b divides a .

Ex. $847|485331$ since $485331 = 573 \cdot 847$

Def. 2.2 A common divisor of two integers a and b is a positive integer d that divides both of them. The greatest common divisor of a and b is the largest positive integer d such that $d|a$ and $d|b$. We write $\gcd(a, b) = d$. The $\gcd(0, 0)$ is not defined.

Ex. $\gcd(12, 18) = 6$ since $6|12$, $6|18$ and there is no larger number with this property. Similarly,

$$\gcd(748, 2024) = 44.$$

How to find the gcd?

~~Divisors of~~ We use division with remainder to describe the Euclidean Algorithm to determine the gcd of two integers.