

Greatest Common Divisor

If a , b , and k are in Z^+ , and $k \mid a$ and $k \mid b$, we say that k is a **common divisor** of a and b . If d is the largest such k , d is called the **greatest common divisor**, or GCD, of a and b , and we write $d = \text{GCD}(a, b)$. This number has some interesting properties. It can be written as a combination of a and b , and it is not only larger than all the other common divisors, it is a multiple of each of them.

Theorem 4 If d is $\text{GCD}(a, b)$, then

- (a) $d = sa + tb$ for some integers s and t . (These are not necessarily positive.)
- (b) If c is any other common divisor of a and b , then $c \mid d$. ●

Proof Let x be the smallest positive integer that can be written as $sa + tb$ for some integers s and t , and let c be a common divisor of a and b . Since $c \mid a$ and $c \mid b$, it follows from Theorem 2 that $c \mid x$, so $c \leq x$. If we can show that x is a common divisor of a and b , it will then be the greatest common divisor of a and b and both parts of the theorem will have been proved. By Theorem 1, $a = qx + r$ with $0 \leq r < x$. Solving for r , we have

$$r = a - qx = a - q(sa + tb) = a - qsa - qtb = (1 - qs)a + (-qt)b.$$

If r is not zero, then since $r < x$ and r is the sum of a multiple of a and a multiple of b , we will have a contradiction to the fact that x is the smallest positive number that is a sum of multiples of a and b . Thus r must be 0 and $x \mid a$. In the same way we can show that $x \mid b$, and this completes the proof. ▼

This proof is more complex than the earlier ones. At this stage you should focus on understanding the details of each step. We will discuss the structure of this proof later.

From the definition of greatest common divisor and Theorem 4(b), we have the following result: Let a , b , and d be in Z^+ . The integer d is the greatest common divisor of a and b if and only if

- (a) $d \mid a$ and $d \mid b$.
- (b) Whenever $c \mid a$ and $c \mid b$, then $c \mid d$.

EXAMPLE 4

- (a) The common divisors of 12 and 30 are 1, 2, 3, and 6, so that

$$\text{GCD}(12, 30) = 6 \quad \text{and} \quad 6 = 1 \cdot 30 + (-2) \cdot 12.$$

- (b) It is clear that $\text{GCD}(17, 95) = 1$ since 17 is prime and $17 \nmid 95$, and the reader may verify that $1 = 28 \cdot 17 + (-5) \cdot 95$. ■

If $\text{GCD}(a, b) = 1$, as in Example 4(b), we say a and b are **relatively prime**.

One remaining question is that of how to compute the GCD conveniently in general. Repeated application of Theorem 1 provides the key to doing this.

We now present a procedure, called the **Euclidean algorithm**, for finding $\text{GCD}(a, b)$. Suppose that $a > b > 0$ (otherwise interchange a and b). Then by Theorem 1, we may write

$$a = k_1b + r_1, \quad \text{where } k_1 \text{ is in } Z^+ \text{ and } 0 \leq r_1 < b. \quad (1)$$

Now Theorem 2 tells us that if n divides a and b , then it must divide r_1 , since $r_1 = a - k_1b$. Similarly, if n divides b and r_1 , then it must divide a . We see that the common divisors of a and b are the same as the common divisors of b and r_1 , so $\text{GCD}(a, b) = \text{GCD}(b, r_1)$.

We now continue using Theorem 1 as follows:

$$\begin{array}{lll}
 \text{divide } b \text{ by } r_1: & b = k_2r_1 + r_2 & 0 \leq r_2 < r_1 \\
 \text{divide } r_1 \text{ by } r_2: & r_1 = k_3r_2 + r_3 & 0 \leq r_3 < r_2 \\
 \text{divide } r_2 \text{ by } r_3: & r_2 = k_4r_3 + r_4 & 0 \leq r_4 < r_3 \\
 \vdots & \vdots & \vdots \\
 \text{divide } r_{n-2} \text{ by } r_{n-1}: & r_{n-2} = k_nr_{n-1} + r_n & 0 \leq r_n < r_{n-1} \\
 \text{divide } r_{n-1} \text{ by } r_n: & r_{n-1} = k_{n+1}r_n + r_{n+1} & 0 \leq r_{n+1} < r_n.
 \end{array} \tag{2}$$

Since $a > b > r_1 > r_2 > r_3 > r_4 > \dots$, the remainder will eventually become zero, so at some point we have $r_{n+1} = 0$.

We now show that $r_n = \text{GCD}(a, b)$. We saw previously that

$$\text{GCD}(a, b) = \text{GCD}(b, r_1).$$

Repeating this argument with b and r_1 , we see that

$$\text{GCD}(b, r_1) = \text{GCD}(r_1, r_2).$$

Upon continuing, we have

$$\text{GCD}(a, b) = \text{GCD}(b, r_1) = \text{GCD}(r_1, r_2) = \dots = \text{GCD}(r_{n-1}, r_n).$$

Since $r_{n-1} = k_{n+1}r_n$, we see that $\text{GCD}(r_{n-1}, r_n) = r_n$. Hence $r_n = \text{GCD}(a, b)$.

EXAMPLE 5

Let a be 190 and b be 34. Then, using the Euclidean algorithm, we

$$\begin{array}{ll}
 \text{divide } 190 \text{ by } 34: & 190 = 5 \cdot 34 + 20 \\
 \text{divide } 34 \text{ by } 20: & 34 = 1 \cdot 20 + 14 \\
 \text{divide } 20 \text{ by } 14: & 20 = 1 \cdot 14 + 6 \\
 \text{divide } 14 \text{ by } 6: & 14 = 2 \cdot 6 + 2 \\
 \text{divide } 6 \text{ by } 2: & 6 = 3 \cdot 2 + 0
 \end{array}$$

so $\text{GCD}(190, 34) = 2$, the last of the nonzero divisors. ■

In Theorem 4(a), we observed that if $d = \text{GCD}(a, b)$, we can find integers s and t such that $d = sa + tb$. The integers s and t can be found as follows. Solve the next-to-last equation in (2) for r_n :

$$r_n = r_{n-2} - k_nr_{n-1}. \tag{3}$$

Now solve the second-to-last equation in (2), $r_{n-3} = k_{n-1}r_{n-2} + r_{n-1}$ for r_{n-1} :

$$r_{n-1} = r_{n-3} - k_{n-1}r_{n-2}$$

and substitute this expression in (3):

$$r_n = r_{n-2} - k_n[r_{n-3} - k_{n-1}r_{n-2}].$$

Continue to work up through the equations in (2) and (1), replacing r_i by an expression involving r_{i-1} and r_{i-2} , and finally arriving at an expression involving only a and b .

EXAMPLE 6

(a) Let $a = 190$ and $b = 34$ as in Example 5. Then

$$\begin{aligned} \text{GCD}(190, 34) &= 2 = 14 - 2(6) \\ &= 14 - 2[20 - 1(14)] & 6 &= 20 - 1 \cdot 14 \\ &= 3(14) - 2(20) \\ &= 3[34 - 1(20)] - 2(20) & 14 &= 34 - 1 \cdot 20 \\ &= 3(34) - 5(190 - 5 \cdot 34) & 20 &= 190 - 5 \cdot 34 \\ &= 28(34) - 5(190) \end{aligned}$$

Hence $s = -5$ and $t = 28$. Note that the key is to carry out the arithmetic only partially.

(b) Let $a = 108$ and $b = 60$. Then

$$\begin{aligned} \text{GCD}(108, 60) &= 12 = 60 - 1(48) \\ &= 60 - 1[108 - 1(60)] & 48 &= 108 - 1 \cdot 60 \\ &= 2(60) - 108. \end{aligned}$$

Hence $s = -1$ and $t = 2$. ■

Theorem 5 If a and b are in Z^+ , then $\text{GCD}(a, b) = \text{GCD}(b, b \pm a)$. ●

Proof If c divides a and b , it divides $b \pm a$, by Theorem 2. Since $a = b - (b - a) = -b + (b + a)$, we see, also by Theorem 2, that a common divisor of b and $b \pm a$ also divides a and b . Since a and b have the same common divisors as b and $b \pm a$, they must have the same greatest common divisor. ▼

This is another direct proof, but one that uses a previous theorem as well as definitions.