

Definition: An integer b is **divisible** by a nonzero integer a if there is an integer c such that $ac = b$.

Note: Saying that b is divisible by a is equivalent to saying any of the following:

a is a **divisor** of b .

a **divides** b .

a is a **factor** of b .

Notation: $a|b$ denotes that a divides b .

Theorem 1: For any integers a , b , and c :

- a.** $a \mid 0$, $1 \mid a$, and $a \mid a$.
- b.** $a \mid 1$ if and only if $a = \pm 1$.
- c.** If $a \mid b$ and $c \mid d$, then $ac \mid bd$.
- d.** If $a \mid b$ and $b \mid c$, then $a \mid c$.
- e.** $a \mid b$ and $b \mid a$ if and only if $a = \pm b$.
- f.** If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for any integers x and y .

Some proofs of Theorem 1

Th 1a: $a|0$, $1|a$, and $a|a$.

Recall: $a|b \Leftrightarrow ac = b$ for some integer c .

Proof: $a \cdot 0 = 0$, $1 \cdot a = a$, and $a \cdot 1 = a$.

So it follows from the def. of “is a divisor of” that $a|0$, $1|a$, and $a|a$.

Th 1b: $a|1$ if and only if $a = \pm 1$.

Proof: By the definition of “is a divisor of,”
 $a|1 \Rightarrow ac = 1$ for some integer c .

But the only *integers* whose product is 1 are $1 \cdot 1$ and $(-1) \cdot (-1)$. So $a = \pm 1$.

On the other hand,

$$a = \pm 1 \Rightarrow a \cdot (\pm 1) = 1 \Rightarrow a|1.$$

Th 1d: If alb and bqc , then alc .

Scratch work:

$$\begin{aligned} alb \text{ and } bqc &\Rightarrow ap = b \text{ and } bq = c \\ &\Rightarrow a(pq) = (ap)q = bq = c \\ &\Rightarrow alc. \end{aligned}$$

Th 1d: If $a|b$ and $b|c$, then $a|c$.

Proof: By the def. of “is a divisor of” there are integers p and q such that

$$\begin{aligned} a|b \text{ and } b|c &\Rightarrow ap = b \text{ and } bq = c \\ &\Rightarrow a(pq) = (ap)q = bq = c \end{aligned}$$

It now follows from the def. of “is a divisor of that $a|c$.

Th 1e: alb and bla if and only if $a = \pm b$.

Sketch of Proof in one direction:

$$alb \text{ and } bla \Rightarrow ap = b, bq = a \text{ and } b \neq 0$$

$$\Rightarrow b(qp) = (bq)p = ap = b$$

$$\Rightarrow qp = 1$$

$$\Rightarrow q = \pm 1$$

$$\Rightarrow a = b \cdot (\pm 1) = \pm b$$

Greatest Common Divisor

d is the **greatest common divisor** of integers a and b if d is the largest integer which is a common divisor of both a and b .

Notation: $d = \gcd(a, b)$

Example: ± 2 , ± 7 , and ± 14 are the only integers that are common divisors of both 42 and 56. Since 14 is the largest, $\gcd(42, 56) = 14$.

Use of the gcd

Reducing fractions

$$\text{Ex. } \frac{42}{56} = \frac{14 \cdot 3}{14 \cdot 4} = \frac{3}{4}$$

Not all fractions are easily reduced.

$$\text{Ex. } \frac{8051}{8633}$$

The Division Algorithm

For integers a and b , with $b > 0$, there exist integers q and r such that

$$a = qb + r \quad \text{and} \quad 0 \leq r < b.$$

$$\begin{array}{r} q \text{ R. } r \\ b \overline{) a} \\ \underline{-bq} \\ r \end{array}$$

$$\begin{array}{r} 2 \text{ R. } 3 \\ 2 \overline{) 7} \\ \underline{-4} \\ 3 \end{array}$$

$$\begin{array}{r} 4 \text{ R. } -1 \\ 2 \overline{) 7} \\ \underline{-8} \\ -1 \end{array}$$

$$a = bq + r$$

$$7 = 2 \cdot 2 + 3$$

$$7 = 2 \cdot 4 + -1$$

Euclidean Algorithm

To find $\gcd(a, b)$ where $b < a$:

Divide b into a and let r_1 be the remainder.

Divide r_1 into b and let r_2 be the remainder.

Divide r_2 into r_1 and let r_3 be the remainder.

Continue to divide the remainder into the divisor until you get a remainder of zero.

$\gcd(a, b) =$ the last nonzero remainder.

Find $\gcd(8633, 8051)$

$8051 \overline{)8633} \quad 1 \text{ R.}582 \quad 582 \overline{)8051} \quad 13 \text{ R.}485 \quad 485 \overline{)582} \quad 1 \text{ R.}97 \quad 97 \overline{)485} \quad 5 \text{ R.}0$

$\gcd = \text{last nonzero remainder}$

$$\frac{8051}{8633} = \frac{97 \cdot 83}{97 \cdot 89} = \frac{83}{89}$$

Theorem 2

For any nonzero integers a and b , there exist integers x and y such that

$$\gcd(a, b) = ax + by.$$

Here's how you use the Euclidean Algorithm to write $\gcd(8633, 8051)$ as a linear combination of 8633 and 8051.

- Use the Euclidean Algorithm to find $\gcd(8633, 8051)$.

$$8051 \overline{)8633} \quad 1 \text{ R.}582$$

$$582 \overline{)8051} \quad 13 \text{ R.}485$$

$$485 \overline{)582} \quad 1 \text{ R.}97$$

$$97 \overline{)485} \quad 5 \text{ R.}0$$

- Solve each division problem, except the last one, for the remainder ($r = a - bq$).
Take note of the quotient in each solution.

$$8051 \overline{)8633} \quad \begin{array}{l} 1 \\ \hline \end{array} \text{ R.582} \quad \Rightarrow \quad 582 = 8633 - 1 \cdot 8051$$

$$582 \overline{)8051} \quad \begin{array}{l} 13 \\ \hline \end{array} \text{ R.485} \quad \Rightarrow \quad 485 = 8051 - 13 \cdot 582$$

$$485 \overline{)582} \quad \begin{array}{l} 1 \\ \hline \end{array} \text{ R.97} \quad \Rightarrow \quad 97 = 582 - 1 \cdot 485$$

$$97 \overline{)485} \quad \begin{array}{l} 5 \\ \hline \end{array} \text{ R.0}$$

- Use these equations in reverse order to find the linear combination.

$$1: 582 = 8633 - 1 \cdot 8051$$

$$2: 485 = 8051 - 13 \cdot 582$$

$$3: 97 = 582 - 1 \cdot 485$$

$$97 = 582 - 1 \cdot 485$$

Eq. 3

$$= 582 - 1 \cdot (8051 - 13 \cdot 582)$$

Eq. 2

$$= 14 \cdot 582 - 1 \cdot 8051$$

Simp.

$$= 14 \cdot (8633 - 1 \cdot 8051) - 1 \cdot 8051$$

Eq. 1

$$= 14 \cdot 8633 + (-15) \cdot 8051$$

Simp.