The greatest common divisor (gcd).

\[ a, b \] integers, not both 0.

\[ \text{gcd} (a, b) = \text{largest integer that divides both } a, b. \]

Simple properties:

1. If \( a \neq 0 \), then \( \text{gcd} (a, 0) = |a| \).
2. \( \text{gcd} (a, b) \geq 1 \)
3. If \( \text{gcd} (a, b) = d \), then \( \text{gcd} \left( \frac{a}{d}, \frac{b}{d} \right) = 1 \).

Proof of (1): common divisors of \( a, 0 \) are the divisors of \( a \). The largest of these is \( |a| \).

Proof of (2): 1 divides both \( a, b \). Thus \( \text{gcd} (a, b) \geq 1 \).

Proof of (3): Suppose \( \text{gcd} \left( \frac{a}{d}, \frac{b}{d} \right) = e \geq 1 \)

\[ \text{Need to show: } e = 1. \]
Then \( \frac{a}{d} = e \frac{k}{d} \), \( \frac{b}{d} = e \frac{m}{d} \) for some integers \( k, m \). Now

\[
a = (de)k \quad \Rightarrow \quad \text{de is a common divisor of } a \text{ and } b
\]

\[
b = (de)m
\]

\[
\Rightarrow \quad \text{de} \leq \gcd(a, b) = d
\]

Thus \( \text{de} \leq d \Rightarrow e \leq 1 \). Since we also know that \( e \geq 1 \), we conclude that \( e = 1 \).

Q.E.D.

An integer linear combination of \( a \) and \( b \) is an integer of the form \( xa + yb \), where \( x, y \) are integers.

Example: \( a = 4, b = 10 \). Then

\[
2 = (-2) \cdot 4 + 1 \cdot 10 \quad \text{is an integer linear comb. of } a \text{ and } b.
\]

On the other hand,
1 is not an integer linear combination of 4 and 10, because

\[ x \cdot 4 + y \cdot 10 \] is even for every choice of integers \( x, y \).

Bezout's Theorem: \( \gcd(a, b) \) is the smallest linear combination of \( a \) and \( b \).

\[ \text{positive} \]

Examples:

(i) \( a = 4, \ b = 10 \)

\[ \gcd(4, 10) = 2. \]

\[ 2 = (2) \cdot 4 + 1 \cdot 10 \]

Other choices of \( x, y \) are possible, e.g.,

\[ 3 \cdot 4 + (-1) \cdot 10 = 2. \]

(ii) \( a = 9, \ b = 15 \)

\[ \gcd(9, 15) = 3 \]

\[ 9x + 15y = 3 \] for \( x = 2, \ y = -1 \) or \( x = 17, \ y = -10 \).
Bezout's Theorem (cleaner statement)

\(\gcd(a, b)\) is the smallest positive number of the form \(ax + by\) where \(x, y\) are integers.

Proof: Let \(S\) be the set of positive integers of the form \(ax + by\), where \(x, y\) are integers. By well ordering principle, \(S\) has a minimal element. Denote this element by \(d\). We will show that

1. \(\gcd(a, b)\) divides \(d\)
2. \(d\) divides both \(a\) and \(b\).

Thus (1) and (2) together give
\(\gcd(a, b) = d\), which is what we want to prove.
(1) is easy: \( \gcd(a, b) | a \) \\
\( \gcd(a, b) | b \)

\[ \Rightarrow \gcd(a, b) | ax + by \text{ for any integers } x, y \Rightarrow \gcd(a, b) \text{ divides } d. \]

Let us now prove (2) by showing that \( d | a \). The same argument will show that \( d | b \). Divide \( a \) by \( d \) with remainder: \( a = dq + r \) where \( 0 \leq r \leq d-1 \). Our goal is to show that \( r = 0 \). Recall that \( d = x_0 a + y_0 b \) is a linear combination of \( a, b \) with integer coefficients. Then \( r = \frac{a - dq}{x_0 a + y_0 b} = (1 - qx_0) a + (-qy_0) b \)
We have thus found a linear combination \( r \) of \( a, b \) that is \( \leq d-1 \). Since \( d \) is the smallest positive linear combination of \( a \) and \( b \), we conclude that \( r \) cannot be positive. Recall that \( 0 \leq r \leq d-1 \). Thus \( r = 0 \), as desired. This completes the proof of (2) and thus of Bezout's Theorem. Q.E.D.

**Corollary 1:** Any common divisor \( e \) of \( a \) and \( b \) divides \( \text{gcd}(a, b) \).

**Proof:** By Bezout, \( \text{gcd}(a, b) = xa + yb \) for some integers \( x, y \). Since \( e \mid a \) and \( e \mid b \), we conclude that \( e \mid xa + yb = \text{gcd}(a, b) \). Q.E.D.
Corollary 2: Let $a, b, c$ be integers, $(a, b) \neq (0, 0)$. The equation $ax + by = c$ has an integer solution $(x, y)$ if and only if $\gcd(a, b)$ divides $c$.

Proof: $\gcd(a, b)$ divides every integer of the form $ax + by$ where $x, y$ are integers.

If $\gcd(a, b)$ does not divide $c$, then $ax + by$ cannot be equal to $c$ for any integers $x, y$. In other words, in this case our equation has no solutions.
Conversely, suppose \( \gcd(a, b) \mid c \), i.e., \( \gcd(a, b) = d \) and \( c = dn \) for some integer \( n \). We want to show that \( ax + by = c \) for some integers \( x, y \). By Bézout's theorem, we know that

\[ ax_0 + by_0 = d \]

for some integers \( x_0, y_0 \). Multiplying both sides by \( n \), we obtain

\[ a(nx_0) + b(ny_0) = dn \]

or

\[ a(nx_0) + b(ny_0) = c \]

Thus \( (x, y) = (nx_0, ny_0) \) is an integer solution to \( ax + by = c \).

Q.E.D.
The Euclidean algorithm is an algorithm for computing $\gcd(a, b)$ where $a \geq b \geq 0$, $(a, b) \neq (0, 0)$.

Key observation

Lemma: $\gcd(a, b) = \gcd(a + nb, b)$ for any integer $n$.

Proof: Let $a' = a + nb$.

Then any common divisor of $a$ and $b$ also divides $a'$ and $b$.

Any common divisor of $a'$ and $b$ also divides $a = a' - nb$ and $b$.

In other words, $(a, b)$ and $(a', b)$ have the same common divisors $\Rightarrow$ same gcd. Q.E.D.
Corollary: Suppose $r$ is the remainder of division of $a$ by $b$. Then $\gcd(a, b) = \gcd(b, r)$.

To prove Corollary, write

$$a = bq + r$$

and apply Lemma with $n = -q$:

$$\gcd(a, b) = \gcd(a + nb, b)$$

$$= \gcd(a - qb, b) = \gcd(r, b)$$

$$= \gcd(b, r).$$

The Euclidean algorithm is based on applying this corollary recursively.

Note that $0 \leq r \leq b-1$, so when we replace $(a, b)$ with $(b, r)$, we're working with smaller numbers.
The algorithm terminates when we reduce to a pair of the form $(d, 0)$. At that point we know that $gcd(a, b) = gcd(b, r) = \ldots = gcd(d, 0) = d$

Examples: (1) $a = 30, \ b = 18$

**Step 1**: Divide 30 by 18:

$30 = 18 \cdot 1 + 12$  Replace $(30, 18)$ by $(18, 12)$

**Step 2**: Divide 18 by 12

$18 = 12 \cdot 1 + 6$  Replace $(18, 12)$ by $(12, 6)$

**Step 3**: Divide 12 by 6

$12 = 6 \cdot 2 + 0$  Replace $(12, 6)$ by $(6, 0)$

$gcd(30, 18) = gcd(18, 12) = gcd(12, 6) = gcd(6, 0) = 6$
Example 2  \[ a = 3600 \]
\[ b = 1065 \]

Once again we divide \( a \) by \( b \) with remainder: \( a = bq + r \) and replace \((a,b)\) by \((b,r)\).

\[ 3600 = 1065 \cdot 3 + 405 \]

Replace \((3600,1065)\) by \((1065,405)\).

Proceed recursively:

\[ \gcd(3600,1065) = \gcd(1065,405) \]
\[ = \gcd(405,255) = \gcd(255,150) \]
\[ = \gcd(150,105) = \gcd(105,45) \]
\[ = \gcd(45,15) = \gcd(15,0) = 15 \]

How many steps are involved in computing \( \gcd(a,b) \)?
Expect the no. of steps to increase as $a, b$ get larger. The question is: at what rate does the no. of steps increase?

**Lemma:** Let $a \geq b > 0$ be integers. Divide $a$ by $b$ with remainder: $a = bq + r$, $0 \leq r \leq b-1$. Then $r < \frac{a}{2}$.

$\gcd(a, b) = \gcd(b, r) = \gcd(r, r_i)$

where $r_i$ is the remainder of division of $b$ by $r$.

**Proof of Lemma:** Consider two cases.

Case 1: $b \leq \frac{a}{2}$. In this case $r < b \leq \frac{a}{2}$. 
Case 2: $b > \frac{a}{2}$. In this case $q = 1$ and $r = a - b$. Note that $a - b < \frac{a}{2} < b$

\[
\begin{align*}
a &= b \cdot 1 + (a - b) \\
&= \underbrace{\frac{a}{q}}_{\text{Example: } a = 100} + \underbrace{(a - b)}_{\text{Case 1: } b \leq 50} \\
&= \underbrace{r}_{\text{Case 2: } b > 50} \frac{a}{2}
\end{align*}
\]

$r = a - b < \frac{a}{2}$, as desired. Q.E.D.

**Theorem:** The no. of steps required to compute gcd $(a, b)$ using Euclidean algorithm is at most $2 \cdot \log_2(a)$.

**Proof:** By Lemma the larger of the two numbers $(a, b)$ decreases by at least a factor of 2 after 2 steps. After $2n$ steps, this number will be at most $\frac{a}{2^n}$. If $2n$ steps are required, then $\frac{a}{2^n} \geq 1$, i.e., $a \geq 2^n$
or equivalently, \( n \leq \lceil \log_2(a) \rceil \). Thus \# of steps is \( \leq 2n \leq 2 \log_2(a) \). Q.E.D.

This shows that the no. of steps in Euclidean algorithm is logarithmic in \( a \).

The book proves a different estimate called Lame' s Theorem.

Suppose \( a \geq b \geq 0, (a, b) \neq (0, 0) \). Then the no. of steps required to compute \( \gcd(a, b) \) using the Euclidean algorithm is at most \( 5d \), where \( d \) is the number of digits in \( b \).
Let us compare our bound to Lame's. Our bound

\[ \# \, \text{of steps} \leq 2 \log_2(a) = 2 \frac{\log_{10}(a)}{\log_{10}(2)} \approx 6.64 \log_{10}(a) < 6.64 \cdot \# \, \text{of digits of } a. \]

Lame's bound:

\[ \# \, \text{of steps} \leq 5(\# \, \text{of digits of } b) \]

Conclusion: Lame's bound is a bit better.

Example: \( a = 50771 \)
\( b = 4326 \)
\( \gcd(a, b) = 7. \)
Euclidean alg. takes 10 steps.
Our estimate for no. of steps is \( 2 \log_2(a) \approx 31.3 \)
Lame's estimate: \( s \cdot (\text{no. of digits in } b) = 20 \).