For integers $a, b$, not both zero, their greatest common divisor, $\gcd(a, b)$, is the largest positive integer that divides both $a$ and $b$. We first prove that $\gcd(a, b)$ is also the smallest positive integer that can be expressed as a linear combination of $a, b$. That is,

$$\gcd(a, b) = \min\{n \in \mathbb{N} : n = ax + by \text{ for some } x, y \in \mathbb{Z}\}.$$ 

For example, if $a = 4$ and $b = 6$, we can look at the table of all possible numbers of the form $ax + by = 4x + 6y$, where $x, y$ are integers.

<table>
<thead>
<tr>
<th>$x$ \ $y$</th>
<th>$-3$</th>
<th>$-2$</th>
<th>$-1$</th>
<th>$0$</th>
<th>$1$</th>
<th>$2$</th>
<th>$3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$-3$</td>
<td>$-30$</td>
<td>$-24$</td>
<td>$-18$</td>
<td>$-12$</td>
<td>$-6$</td>
<td>$0$</td>
<td>$6$</td>
</tr>
<tr>
<td>$-2$</td>
<td>$-26$</td>
<td>$-20$</td>
<td>$-14$</td>
<td>$-8$</td>
<td>$-2$</td>
<td>$4$</td>
<td>$10$</td>
</tr>
<tr>
<td>$-1$</td>
<td>$-22$</td>
<td>$-16$</td>
<td>$-10$</td>
<td>$-4$</td>
<td>$2$</td>
<td>$8$</td>
<td>$14$</td>
</tr>
<tr>
<td>$0$</td>
<td>$-18$</td>
<td>$-12$</td>
<td>$-6$</td>
<td>$0$</td>
<td>$6$</td>
<td>$12$</td>
<td>$18$</td>
</tr>
<tr>
<td>$1$</td>
<td>$-14$</td>
<td>$-8$</td>
<td>$-2$</td>
<td>$4$</td>
<td>$10$</td>
<td>$16$</td>
<td>$22$</td>
</tr>
<tr>
<td>$2$</td>
<td>$-10$</td>
<td>$-4$</td>
<td>$2$</td>
<td>$8$</td>
<td>$14$</td>
<td>$20$</td>
<td>$26$</td>
</tr>
<tr>
<td>$3$</td>
<td>$-6$</td>
<td>$0$</td>
<td>$6$</td>
<td>$12$</td>
<td>$18$</td>
<td>$24$</td>
<td>$30$</td>
</tr>
</tbody>
</table>

The smallest positive integer is $2 = \gcd(4, 6)$. To see that this is true in general, suppose that the smallest positive integer of the form $ax + by$ is $n_0 = ax_0 + by_0$ and that $d = \gcd(a, b)$. We want to show that $d = n_0$. Clearly, since $d$ divides both $a, b$, we have that $d$ divides $n_0$, which implies that $d \leq n_0$. Next, we use the division algorithm to write $n_0 = qa + r$ and $n_0 = Qb + R$ with $0 \leq r, R < n_0$. Then, $n_0 = ax_0 + by_0$ implies that

$$r = n_0 - qa = a(x_0 - q) + by_0 \quad \text{and} \quad R = n_0 - Qb = ax_0 + b(y_0 - Q),$$

so $r, R$ are of the form $ax + by$ for some integers $x, y$. Since $n_0$ is the smallest positive integer of this form, we see that $r = R = 0$. Therefore, $n_0$ is a common divisor of both $a$ and $b$, hence $n_0 \leq d$.

**Bezout’s identity.** As a corollary of the argument above, we get the following theorem, known as Bezout’s identity.

Given integers $a, b$, not both zero, there exist integers $x, y$ such that

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

**Euclidean algorithm.** The Euclidean algorithm is an efficient way to compute the greatest common divisor between two integers and also to find a solution $x, y$ to Bezout’s identity. Given integers $a, b$, you perform the division algorithm on $a, b$,

$$a = qb + r;$$

if $r = 0$, you are done; otherwise, replace $a, b$ by $b, r$ and perform the division algorithm again. By repeating this loop, you eventually get a remainder of 0 because the remainders are a decreasing sequence of positive integers. Essentially, the Euclidean algorithm is just repeated use of the division algorithm.

For example, if we start with $a = 92$ and $b = 78$, the Euclidean algorithm gives:

$$
\begin{align*}
92 &= 1 \cdot 78 + 14 \\
78 &= 5 \cdot 14 + 8 \\
14 &= 1 \cdot 8 + 6 \\
8 &= 1 \cdot 6 + 2 \\
6 &= 3 \cdot 2 + 0.
\end{align*}
$$

We stop when we finally get a remainder of 0.

As a first application of the Euclidean algorithm, we get the following theorem.

The last nonzero remainder in the Euclidean algorithm on $a, b$ is $\gcd(a, b)$. 
To prove this, we note that if \( a = qb + r \), then any common divisor of \( b \), \( r \) is also a divisor of \( a \); in addition, if \( r = a - qb \), then any common divisor of \( a \), \( b \) is also a divisor of \( r \). Therefore, anytime the division algorithm is invoked, we have \( \gcd(a, b) = \gcd(b, r) \). Suppose now that the Euclidean algorithm on \( a \), \( b \) is given by

\[
\begin{align*}
    a &= q_1 b + r_1 \\
    b &= q_2 r_1 + r_2 \\
    r_1 &= q_3 r_2 + r_3 \\
    &\vdots \\
    r_{n-2} &= q_n r_{n-1} + r_n \\
    r_{n-1} &= q_{n+1} r_n + 0.
\end{align*}
\]

Repeated use of the fact proved above yields

\[
\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \gcd(r_2, r_3) = \cdots = \gcd(r_{n-1}, r_n).
\]

Since the final division shows that \( r_n \) is a divisor of \( r_{n-1} \), we conclude that

\[
\gcd(a, b) = \gcd(r_{n-1}, r_n) = \gcd(a, b).
\]

In the example above, we conclude that \( \gcd(92, 78) = \gcd(78, 14) = \gcd(14, 8) = \gcd(6, 2) = 2 \).

As a second application of the Euclidean algorithm, we find a solution \( x, y \) to \( ax + by = \gcd(a, b) \). Starting at the second-to-last equation in the Euclidean algorithm, we solve for each of the remainders and then systematically perform substitutions. The easiest way to show this is with an example. For \( a = 92 \) and \( b = 78 \), we do the Euclidean algorithm as above and then solve for the remainders to get

\[
\begin{align*}
    2 &= 8 - 6 \\
    6 &= 14 - 8 \\
    8 &= 78 - 5 \cdot 14 \\
    14 &= 92 - 78.
\end{align*}
\]

Substituting the second equation into the first and then collecting like terms gives us

\[
2 = 8 - 6 = 8 - (14 - 8) = -14 + 2 \cdot 8.
\]

Substituting the third equation into this new one gives us

\[
2 = -14 + 2 \cdot 8 = -14 + 2(78 - 5 \cdot 14) = 2 \cdot 78 - 11 \cdot 14.
\]

Finally, substituting the fourth equation into the new one gives us

\[
2 = 2 \cdot 78 - 11 \cdot 14 = 2 \cdot 78 - 11(92 - 78) = -11 \cdot 92 + 13 \cdot 78.
\]

Therefore \( x = -11 \) and \( y = 13 \) is a solution to \( 92x + 78y = \gcd(92, 78) \). Indeed, \( 92 \cdot -11 + 78 \cdot 13 = 1012 \) and \( 78 \cdot 13 = 1014 \), so \( 92(-11) + 78(13) = 2 \).

We conclude this section with three statements, which will be proved in the exercises.

1. If \( D \) is a common divisor of \( a \), \( b \), then \( D \) is a divisor of \( \gcd(a, b) \).
2. If \( M \) is a common multiple of \( a \), \( b \), then \( M \) is a multiple of \( \text{lcm}(a, b) \).
3. For any integers \( a \), \( b \), not both zero, \( ab = \gcd(a, b) \cdot \text{lcm}(a, b) \).

In particular, to find the least common multiple of two integers \( a \), \( b \), first use the Euclidean algorithm to find the greatest common divisor, say \( d = \gcd(a, b) \). The third statement in the list will mean that \( \text{lcm}(a, b) = \frac{ab}{d} \), which you can easily compute as \( \frac{a}{d} \cdot b \) or \( \frac{b}{d} \cdot a \). For example,

\[
\text{lcm}(92, 78) = \frac{92}{2} \cdot 78 = 46 \cdot 78 = 3588.
\]
Exercises

1. For each of the following, perform the Euclidean algorithm on \( a, b \), find \( \gcd(a, b) \) and \( \text{lcm}(a, b) \), and find a solution \( x, y \) to \( ax + by = \gcd(a, b) \).

   (a) \( a = 1234, b = 234 \)  \hspace{1cm}  (d) \( a = 121, b = 23 \)

   (b) \( a = 505, b = 75 \)  \hspace{1cm}  (e) \( a = 3873, b = 2532 \)

   (c) \( a = 201, b = 44 \)  \hspace{1cm}  (f) \( a = 21, b = 13 \)

2. Let \( a, b \) be nonzero integers with \( d = \gcd(a, b) \) and suppose that \( x = x_0 \) and \( y = y_0 \) is a solution to \( ax + by = d \). Verify that

\[
x = x_0 + \frac{b}{d}k \quad \text{and} \quad y = y_0 - \frac{a}{d}k
\]

is also a solution to \( ax + by = d \), no matter what integer \( k \) is used.

3. For this problem, let \( a, b \) be nonzero integers with \( d = \gcd(a, b) \) and \( m = \text{lcm}(a, b) \). We will prove the three statements at the end of the section.

   (a) If \( D \) is a common divisor of both \( a \) and \( b \), prove that \( D \) is a divisor of \( d \).

   (Hint: use Bezout’s identity to write \( ax + by = d \) for some integers \( x \) and \( y \).)

   (b) If \( M \) is a common multiple of both \( a \) and \( b \), prove that \( M \) is a multiple of \( m \).

   (Hint: use the division algorithm to write \( M = qm + r \); then show that \( r \) must be a common multiple of \( a \) and \( b \); we know that \( r = 0 \) or that \( 0 < r < m \); explain why it is impossible that \( 0 < r < m \); conclude that \( r = 0 \).)

   (c) Prove that \( ab \geq dm \).

   (Hint: show that \( \frac{ab}{d} \) is a common multiple of both \( a \) and \( b \); then conclude that \( \frac{ab}{d} \) is greater than or equal to the least common multiple. Why does this give the inequality desired?)

   (d) Prove that \( ab \leq dm \).

   (Hint: use Bezout’s identity to write \( ax + by = d \) for some integers \( x, y \); then multiply both sides by \( m \); explain by the left-hand side is divisible by \( ab \); then conclude that the right-hand side must be divisible by \( ab \). Why does this give the inequality desired?)
Answers

1. (a) \( \gcd(1234, 234) = 2 \), \( \text{lcm}(1234, 234) = 144, 378 \), and \( 1234(11) + 234(-58) = 2 \).

(b) \( \gcd(505, 75) = 5 \), \( \text{lcm}(505, 75) = 7575 \), and \( 505(-4) + 75(27) = 5 \).

(c) \( \gcd(201, 44) = 1 \), \( \text{lcm}(201, 44) = 8844 \), and \( 201(-7) + 44(32) = 1 \).

(d) \( \gcd(121, 23) = 1 \), \( \text{lcm}(121, 23) = 2783 \), and \( 121(4) + 23(-21) = 1 \).

(e) \( \gcd(3873, 2532) = 3 \), \( \text{lcm}(3873, 2532) = 3, 268, 812 \), and \( 3873(287) + 2532(-439) = 3 \).

(f) \( \gcd(21, 13) = 1 \), \( \text{lcm}(21, 13) = 273 \), and \( 21(5) + 13(-8) = 1 \).

2. We assume that \( x = x_0, y = y_0 \) is a solution to \( ax + by = d \), i.e., that \( ax_0 + by_0 = d \). For \( x = x_0 + \frac{b}{d} k \) and \( y = y_0 - \frac{a}{d} k \), we get

\[
ax + by = a(x_0 + \frac{b}{d} k) + b(y_0 - \frac{a}{d} k) = ax_0 + by_0 = d,
\]

so these values are solutions as well.

3. (a) Suppose that \( D \) is a common divisor of \( a, b \), i.e., that \( a = Dk \) and \( b = Dl \). Since \( d = \gcd(a, b) \), we know that there exist integers \( x, y \) such that \( ax + by = d \). Therefore,

\[
(Dk)x + (Dl)y = d \quad \rightarrow \quad D(kx + \ell y) = d,
\]

so \( D \) is a divisor of \( d \).

(b) Suppose that \( M \) is a common multiple of \( a, b \). Since \( m \) is the least common multiple, we know that \( m \leq M \). We use the division algorithm to write \( M = qm + r \). We can write \( M = ka \) and \( m = \ell a \), so

\[
r = M - qm = ka - q\ell a = (k - q\ell)a,
\]

so \( r \) is a multiple of \( a \). We can also write \( M = rb \) and \( m = sb \), so

\[
r = M - qm = rb - qsb = (r - qs)b,
\]

so \( r \) is a multiple of \( b \). If \( 0 < r < m \), then \( r \) is a common multiple of \( a, b \) which is smaller than the least common multiple, which is impossible. Therefore, \( r = 0 \), so \( M = qm \), which means that \( M \) is a multiple of \( m \).

(c) We can write \( a = dk \) and \( b = dl \). Then

\[
\frac{ab}{d} = \frac{(dk)b}{d} = kb \quad \text{and} \quad \frac{ab}{d} = \frac{a(dl)}{d} = al.
\]

So \( \frac{ab}{d} \) is a common multiple of \( a, b \). Since \( m \) is the least common multiple, we know that \( \frac{ab}{d} \geq m \). Multiplying both sides by the positive integer \( d \) gives us the inequality \( ab \geq dm \).

(d) We use Bezout’s identity to write \( ax + by = d \) for some integers \( x, y \). Then we multiply both sides by \( m \) to get \( amx + bmy = dm \). We know that \( m = ka \) and \( m = \ell b \) for some integers \( k, \ell \). If we substitute \( m = \ell b \) into the first instance and \( m = ka \) into the second instance, we get

\[
a(\ell b)x + b(ka)y = dm \quad \rightarrow \quad ab(\ell x + ky) = dm.
\]

Therefore, \( ab \) is divisible by \( dm \), so \( ab \geq dm \).