Back-substitution examples

Joshua Maglione

September 22, 2026

The purpose of **back-substitution** is to express the greatest common divisor of two integers a and b as an integer linear combination

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

The Euclidean algorithm first finds the greatest common divisor, and then the equations are used in reverse order to find suitable integers x and y—hence the name.

Example 1

Find x and y such that $252x + 198y = \gcd(252, 198)$.

Step 1: Apply the Euclidean algorithm

Divide repeatedly, keeping track of the remainders:

$$\begin{aligned} 252 &= 1(198) + 54, && (1) \\ 198 &= 3(54) + 36, && (2) \\ 54 &= 1(36) + 18, && (3) \\ 36 &= 2(18) + 0. && (4) \end{aligned}$$

We have the following sequence of remainders (starting with b): $198, 54, 36, 18, 0$. The last non-zero remainder is 18. Therefore,

$$\gcd(252, 198) = 18.$$

Step 2: Work backwards

Start with the equation that produced the gcd, which is Equation (3), and rewrite it so that the gcd is isolated:

$$18 = 54 - 36. \tag{5}$$

Rewriting Equation (2) of the Euclidean algorithm, we have

$$36 = 198 - 3(54). \tag{6}$$

Now we use Equation (6) in Equation (5), replacing the 36:

$$\begin{aligned} 18 &= 54 - \big(198 - 3(54)\big) \\ &= 54 - 198 + 3(54) \\ &= 4(54) - 198. \end{aligned}$$

We are going to repeat this process.

We left off with the following equation:

$$18 = 4(54) - 198. \tag{7}$$

In the previous part, we used the work we did in Step 1 to replace 36 with a combination of 54 and 198. Now we will replace the next smallest remainder, 54, using the work from Step 1. From Equation (1),

$$54 = 252 - 198. \tag{8}$$

Like last time, we use Equation (8) in Equation (7) by replacing 54:

$$\begin{aligned} 18 &= 4(252 - 198) - 198 \\ &= 4(252) - 4(198) - 198 \\ &= 4(252) - 5(198). \end{aligned}$$

Now we have arrived at the equation we are after:

$$252(4) + 198(-5) = 18.$$

Therefore, one suitable pair (x, y) is

$$\boxed{x = 4, \qquad y = -5.}$$

Verification

Quick sanity check:

$$252(4) + 198(-5) = 1008 - 990 = 18 = \gcd(252, 198).$$

Key idea

When performing back-substitution:

1. Find the gcd using the Euclidean algorithm.
2. Start with the equation containing the last non-zero remainder.
3. Replace each remainder using the equation immediately above it.
4. Continue until only the original integers a and b remain.
5. Read off the coefficients x and y from

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

Example 2

Find x and y such that $414x + 662y = \gcd(414, 662)$. Try this yourself first! A bare-bones explanation is on the following page.

Step 1: Apply the Euclidean algorithm

$$\begin{aligned}
662 &= 1(414) + 248, \\
414 &= 1(248) + 166, \\
248 &= 1(166) + 82, \\
166 &= 2(82) + 2, \\
82 &= 41(2) + 0.
\end{aligned}$$

Step 2: Work backwards

$$\begin{aligned}
2 &= 166 - 2(248 - 166) \\
&= 166 - 2(248) + 2(166) \\
&= 3(166) - 2(248) \\
&= 3(414 - 248) - 2(248) \\
&= 3(414) - 3(248) - 2(248) \\
&= 3(414) - 5(248) \\
&= 3(414) - 5(662 - 414) \\
&= 3(414) - 5(662) + 5(414) \\
&= 8(414) - 5(662).
\end{aligned}$$

Exercises

1. Use the Euclidean algorithm and back-substitution to find one pair of integers x, y satisfying
$$391x + 299y = 161.$$

2. Find *all* pairs of integers x, y satisfying
$$132x + 84y = 36.$$
[**Hint:** There are infinitely many solutions—you'll want to parametrize them by some integer n.]