

Euclidean Algorithm

The Euclidean algorithm is a systematic method for calculating the greatest common divisor of two integers. The objective of this exercise is to write the user-defined MATLAB script `euclid.m` that implements the Euclidean algorithm.

We'll begin with a theorem.

Let a and b be two integers, at least one of them nonzero. Then there exists a greatest common divisor d of a and b . Moreover, there exist integers m and n such that

$$d = a \times m + b \times n.$$

The Euclidean algorithm might very well be the oldest mathematical algorithm currently in use. Older mathematical algorithms have been found among the Babylonians, but more efficient algorithms have supplanted them.

The Euclidean algorithm calculates the greatest common divisor of a and b in the following manner:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{k-2} &= q_k r_{k-1} + r_k \\ r_{k-1} &= q_{k+1} r_k \end{aligned}$$

The last nonzero remainder r_k is the greatest common divisor of a and b .

For example, calculate the greatest common divisor of 1492 and 1776.

$$\begin{aligned} 1776 &= 1 \times 1492 + 284 \\ 1492 &= 5 \times 284 + 72 \\ 284 &= 3 \times 72 + 68 \\ 72 &= 1 \times 68 + 4 \\ 68 &= 17 \times 4 + 0 \end{aligned}$$

So, the greatest common divisor of 1492 and 1776 is 4.

We can do even better than this because there's a way of recovering both m and n as well. Here's how:

Start with a table whose first row consists of a , 1, and 0 and whose second row is b , 0, and 1, in that order. To calculate the third row of the table, calculate the largest integer q such that $b \times q < a$. Then,

$$\text{Third Row} = \text{First Row} - q \times \text{Second Row}.$$

The fourth row is calculated in exactly the same manner: Let the new value of q equal the largest integer such that q times the first element in Row 3 is less than the first element in Row 2. Then,

$$\text{Fourth Row} = \text{Second Row} - q \times \text{Third Row}.$$

Continue this way until the first element in the last row equals zero. The next-to-last-row contains d , m , and n , in that order.

Here is a table using $a = 1776$ and $b = 1492$.

1776	1	0
1492	0	1
284	1	-1
72	-5	6
68	16	-19
4	-21	25
0	373	-444

So, $d = 4$, $m = -21$, and $n = 25$. You can verify that $-21 \times 1776 + 25 \times 1492 = 5$.

Given two positive integers a and b , write the **R** function `euclid.r` that calculates the greatest common divisor d of a and b and the integers m and n such that $d = m \times a + n \times b$. Also, display the results of the computation.

Here are several examples.

```
> euclid(1776,1492)
[1] 4 -21 25
> euclid(1492,1776)
[1] 4 25 -21
> euclid(168,456)
[1] 24 -8 3
> euclid(130,65)
[1] 65 0 1
> euclid(10,130)
[1] 10 1 0
> euclid(29630,44805)
[1] 5 -809 535
> euclid(44805,24601)
[1] 1 -9752 17761
> euclid(491891400,1138845708)
[1] 468468 1109 -479
```