

Some examples for the Euclidean algorithm

| a | b | q | r |
|-----------|-------|--------|-----------|
| 284 | 220 | 1 | 64 |
| 220 | 64 | 3 | 28 |
| 64 | 28 | 2 | 8 |
| 28 | 8 | 3 | 4 |
| 8 | 4 | 2 | 0 |
| 67890 | 12345 | 5 | 6165 |
| 12345 | 6165 | 2 | 15 |
| 6165 | 15 | 411 | 0 |
| 123456789 | 951 | 129817 | 822 |
| 951 | 822 | 1 | 129 |
| 822 | 129 | 6 | 48 |
| 129 | 48 | 2 | 33 |
| 48 | 33 | 1 | 15 |
| 33 | 15 | 2 | 3 |
| 15 | 3 | 5 | 0 |

Here are three examples with the initial choices of $(a, b) = (284, 220)$, $(67890, 12345)$ and $(123456789, 951)$. One finds q and r by long division. At the next line, take the new a to be the previous b and the new b to be the previous r . Eventually the iteration of this process will yield a value of 0 for the remainder r , at which point the iteration stops, and the greatest common divisor d will be the remainder from the next to last iteration. For the three examples, the greatest common divisors are **4**, **15** and **3** respectively.

One can now work backwards to write $d = sa + tb$ for suitable integers a and b :

$$4 = 28 - 8 \cdot 3, \quad 8 = 64 - 28 \cdot 2, \quad 28 = 220 - 64 \cdot 3, \quad 64 = 284 - 220 \text{ imply}$$

$$28 = 220 - 64 \cdot 3 = 220 - (284 - 220) \cdot 3 = 220 \cdot 4 - 284 \cdot 3$$

$$8 = 64 - 28 \cdot 2 = (284 - 220) - (220 \cdot 4 - 284 \cdot 3) \cdot 2 = 7 \cdot 284 - 9 \cdot 220$$

$$4 = 28 - 8 \cdot 3 = (220 \cdot 4 - 284 \cdot 3) - 3 \cdot (7 \cdot 284 - 9 \cdot 220) = 31 \cdot 220 - 24 \cdot 284$$