



The Euclidean Algorithm

A METHOD FOR FINDING THE GREATEST COMMON DIVISOR FOR TWO LARGE NUMBERS

To be successful using this method you have got to know how to divide. If this is something that you have not done in a while and have forgotten or have never really mastered and have relied on the use of a calculator instead, you will first want to review the “Long Division” algorithm. Presented here is one example:

$$3846 \div 153$$

$$\begin{array}{r}
 25 \text{ R } 21 \\
 \hline
 153 \overline{)3846} \\
 \underline{306} \downarrow \\
 786 \\
 \underline{765} \\
 21
 \end{array}$$

The Algorithm for Long Division

Step 1: Divide
Step 2: Multiply quotient by divisor
Step 3: Subtract result
Step 4: Bring down the next digit
Step 5: Repeat

When there are no more digits to bring down, the final difference is the remainder.

This can be rewritten in the form of what is known as the “Division Algorithm” (although it is not an algorithm):

$$3846 = 153 \cdot 25 + 21 \quad (\text{dividend equals divisor times quotient plus remainder})$$

(note that $0 \leq \text{remainder} \leq \text{divisor}$)

If you need more help with long division, go to You Tube and search “long division.” Work through several examples and make sure you can successfully perform each example viewed on your own.

The greatest common divisor (gcd) of two integers, a and b, is the largest integer that divides evenly into both a and b.

We write $\text{gcd}(a, b)$.

There are three methods for finding the greatest common factor.

Method #1 The “easy” method: Inspection

This involves two numbers that, through experience, are easily grasped, such as 12 and 18.

Start with the smaller of the two numbers, 12. Does this divide into both numbers? (No, it does not divide evenly into 18.)

Since 12 didn't work, try the next largest integer that evenly divides 12 – by inspection that number is easily found to be 6. Does 6 also divide 18? Yes, therefore we are done – we have found the greatest common divisor and it is 6, hence, **gcd(12, 18) = 6**.

Now you try some:

Find the greatest common divisor of each by inspection.

(a) $\text{gcd}(24, 54)$

(b) $\text{gcd}(18, 42)$

Method #2 Prime Factorization Method

The first step is to break each number into its prime factorization, then discern all the factors the two numbers have in common. Multiply these together. The result is the greatest common divisor.

Example 1: Find the $\text{gcd}(168, 180)$

$$168 = 2^3 \cdot 3 \cdot 7 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 7$$

$$180 = 2^2 \cdot 3^2 \cdot 5 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$$

The common factors are $2 \cdot 2 \cdot 3 = 12$, therefore **gcf(168, 180) = 12**.

Example 2: Find the $\text{gcd}(220, 1323)$

$$220 = 2^2 \cdot 5 \cdot 11$$

$$189 = 3^3 \cdot 7$$

Now you try some:

Find the greatest common divisor of each by first finding the prime factorization of each number.

(c) $\text{gcd}(244, 354)$

(d) $\text{gcd}(128, 423)$

Observe that these two numbers have no common factors. So in this case the $\text{gcd}(220, 1323) = 1$ and we say that the two integers are “*relatively prime*”.

Method #3 The Euclidean Algorithm

This method asks you to perform successive division, first of the smaller of the two numbers into the larger, followed by the resulting remainder divided into the divisor of each division until the remainder is equal to zero. At that point, look at the remainder of the previous division – that will be the greatest common divisor.

Example:

Find the $\text{gcd}(1424, 3084)$

WORK SPACE:

① $1424 \overline{)3084}$
 $\underline{-2848}$
 236

② $236 \overline{)1424}$
 $\underline{-1416}$
 8

③ $8 \overline{)236}$
 $\underline{-16}$
 76
 $\underline{-72}$
 4

④ $4 \overline{)8}$
 $\underline{-8}$
 $0 \therefore$

$\text{gcd}(1424, 3084) = 4$

PRESENTATION:

① $3084 = 1424 \cdot 2 + 236$

② $1424 = 236 \cdot 6 + 8$

③ $236 = 8 \cdot 29 + 4$

④ $8 = 4 \cdot 2 + 0$

Hence the $\text{gcd}(1424, 3084) = 4$

Now you try some:

Find the greatest common divisor of each by first finding the prime factorization of each number.

- (e) $\text{gcd}(2415, 3289)$
- (f) $\text{gcd}(4278, 8602)$
- (g) $\text{gcd}(406, 555)$

Note: Gabriel Lamé (1795-1870) found that the number of steps required in the Euclidean Algorithm

is – at most – 5 times the number of digits in the smaller number.

Why does the Euclidean Algorithm work?

The example used to find the $\mathbf{gcd(1424, 3084)}$ will be used to provide an idea as to why the Euclidean Algorithm works. Let \mathbf{d} represent the greatest common divisor. Since this number represents the largest divisor that evenly divides both numbers, it is obvious that $\mathbf{d \mid 1424}$ and $\mathbf{d \mid 3084}$. Hence $\mathbf{d \mid 3084 - 1424}$ in the same way that a numerator of two or more terms is divisible by a factor in the denominator if and only if that factor divides evenly into each individual term in the numerator. Furthermore $\mathbf{d \mid 3084 - 2(1424)}$ or, simplifying the left side, $\mathbf{d \mid 236}$. Consequently we note that \mathbf{d} divides the remainder resulting from the division of the two numbers for which the greatest common factor is being sought. This corresponds to the first long division calculated in the example above.

The problem has now been reduced to a smaller one. We have that $\mathbf{d \mid 1424}$ and $\mathbf{d \mid 236}$. Hence $\mathbf{d \mid 1424 - 236}$, or better yet, $\mathbf{d \mid 1424 - 6(236)}$ which when simplified reveals that $\mathbf{d \mid 8}$. At this point we know that \mathbf{d} must be one of the following values: 1, 2, 4, or 8. Note that 8 is the remainder resulting from the division of the divisor and remainder found in the original division, so it will not be a divisor of both. So we will take the divisor and remainder from the second division to reduce the problem to yet an even smaller one.

Now we know that $\mathbf{d \mid 236}$ and $\mathbf{d \mid 8}$, so $\mathbf{d \mid 236 - 8}$ or $\mathbf{d \mid 236 - 29(8)}$, which leaves us, after calculation, with the fact that $\mathbf{d \mid 4}$. This, of course, corresponds to the third long division performed above.

One last long division reduces the problem one more level – the final level. We have that $\mathbf{d \mid 8}$ and $\mathbf{d \mid 4}$, hence $\mathbf{d \mid 8 - 2(4)}$ or $\mathbf{d \mid 0}$. We can go no further. $\mathbf{d \mid 0}$ does not provide us with any useful information. (Why not?) But $\mathbf{d \mid 4}$, where $\mathbf{4}$ is seen to be the remainder of the last long division, tells us that \mathbf{d} can be 1, 2, or 4. The largest amongst these is $\mathbf{4}$ – so \mathbf{d} must be equal to $\mathbf{4}$ and we are done. We have thus discovered that \mathbf{d} which equals the $\mathbf{gcd(1424, 2084)}$ is equal to $\mathbf{4}$.

Now you try some: Answers

(a) $\gcd(24, 54) = 6$

(b) $\gcd(18, 42) = 6$

(c) $\gcd(244, 354) = 2$

(d) $\gcd(128, 423) = 1$

(e) $\gcd(2415, 3289) = 23$

(f) $\gcd(4278, 8602) = 46$

(g) $\gcd(406, 555) = 1$