The Euclidean algorithm for finding greatest common divisors.

Recall the terminology: given $a, b \in \mathbb{N}$, we can divide b into a as follows:

divisor

remainder

$$a = bq + r \qquad (0 \leq r < b).$$

dividend quotient

Example 1a. Find $\gcd(582, 165)$.

Solution.

Step 1: Divide the smaller number (165) into the larger (582):

$$582 = 165 \cdot 3 + 87.$$

Step 2: Divide the previous remainder into the previous divisor:

$$165 = 87 \cdot 1 + 78.$$

Step 3: Repeat Step 2 until you get a remainder of zero:

$$87 = 78 \cdot 1 + 9$$
$$78 = 9 \cdot 8 + 6$$
$$9 = 6 \cdot 1 + \boxed{3} \longleftarrow$$
$$6 = 3 \cdot 2 + 0.$$

Step 4: The next-to-last remainder (just before remainder zero) is your greatest common divisor.

So

$$\gcd(582,165)=3.$$

Check: $\gcd(582,165)=\gcd(2\cdot 3\cdot 97,\ 3\cdot 5\cdot 11)$
$= 3.$

Example 1b: tracing back from the next-to-last "remainder equation" above, we can express $3=\gcd(582,165)$ as an integer times 582 minus an integer times 165, as follows:

$$\begin{aligned}
3 &= 9-6\cdot 1 && \text{[from next-to-last remainder eq'n]}\\
&= 9-(78-9\cdot 8)\cdot 1 && \text{[rewrite 6 using previous eq'n]}\\
&= 9\cdot 9-78\cdot 1 && \text{[simplify]}\\
&= (87-78\cdot 1)\cdot 9-78\cdot 1 && \text{[rewrite 9 using previous eq'n]}\\
&= 87\cdot 9-78\cdot 10 && \text{[simplify]}\\
&= 87\cdot 9-(165-87\cdot 1)\cdot 10 && \text{[rewrite 78 using previous eq'n]}\\
&= 87\cdot 19-165\cdot 10 && \text{[simplify]}\\
&= (582-165\cdot 3)\cdot 19-165\cdot 10 && \text{[rewrite 87 using previous eq'n]}\\
&= 582\cdot 19-165\cdot 67 && \text{[simplify].}
\end{aligned}$$

Conclusion:

$$\gcd(582,165)=582\cdot 19-165\cdot 67.$$

Example 2.

(a) Show that $\gcd(35,\varphi(39))=1$.

(b) Find $x,y\in\mathbb{Z}$ with

$$35x - \varphi(39)y = 1.$$

Solution.

(a) We have $\varphi(39) = \varphi(3\cdot 13) = 2\cdot 12 = 24$. So we divide 24 into 35, and then proceed as above:

$$35 = 24\cdot 1 + 11$$
$$24 = 11\cdot 2 + 2$$
$$11 = 2\cdot 5 + 1$$
$$2 = 1\cdot 2 + 0$$

so $\gcd(35, \varphi(39)) = 1$.

(b) From the next-to-last remainder equation above,

$$\begin{aligned} 1 &= 11 - 2\cdot 5 \\ &= 11 - (24 - 11\cdot 2)\cdot 5 \\ &= 11\cdot 11 - 24\cdot 5 \\ &= (35 - 24\cdot 1)\cdot 11 - 24\cdot 5 \\ &= 35\cdot 11 - 24\cdot 16. \end{aligned}$$