

1.6: The Euclidean Algorithm

\(\newcommand{\NN}{\mathbb N}\)
\(\newcommand{\RR}{\mathbb R}\)
\(\newcommand{\QQ}{\mathbb Q}\)
\(\newcommand{\ZZ}{\mathbb Z}\)
\(\newcommand{\Cc}{\mathcal C}\)
\(\newcommand{\Dd}{\mathcal D}\)
\(\newcommand{\Ee}{\mathcal E}\)
\(\newcommand{\Ff}{\mathcal F}\)
\(\newcommand{\Kk}{\mathcal K}\)
\(\newcommand{\Mm}{\mathcal M}\)
\(\newcommand{\Pp}{\mathcal P}\)
\(\newcommand{\ind}{\operatorname{ind}}\)
\(\newcommand{\ord}{\operatorname{ord}}\)

In this section, we describe a systematic method that determines the greatest common divisor of two integers, due to Euclid and thus called the Euclidean algorithm.

Lemma \(\PageIndex{1}\)

If \(a,b,q,r\in\ZZ\) and \(a=qb+r\), then \(\gcd(a,b)=\gcd(r,b)\).

Proof

Note that by Theorem 1.5.2, we have \(\gcd(bq+r,b)=\gcd(b,r)\).

Now to the Euclidean algorithm in its general form, which basically states that the greatest common divisor of two integers is the last non-zero remainder of successive divisions.

UC Davis ChemWiki is licensed under a Creative Commons Attribution-Noncommercial-Share Alike 3.0 United States License.

Theorem \(\PageIndex{1}\)

Let \(a,b\in\NN\) and assume \(a\geq b\). Define \(r_0=a\), \(r_1=b\), \(s_0=1\), \(s_1=0\), \(t_0=0\), and \(t_1=1\). Then apply the division algorithm successively to obtain quotients and remainders \(q_j,r_j\in\NN\) satisfying \(r_j=r_{j+1}q_{j+1}+r_{j+2}\) and \(0\leq r_{j+2}<r_{j+1}\) for all \(j=0,1,\dots,n-2\) where \(n\) is defined so that \(r_{n+1}=0\). Along the way, also define \(s_{j+1}=s_{j-1}-q_{j+1}s_j\) and \(t_{j+1}=t_{j-1}-q_{j+1}t_j\). Then \(\gcd(a,b)=r_n= s_{n+1}a+t_{n+1}b\).

Proof

By applying the division algorithm, we see that \[\begin{aligned} r_0&=q_1r_1+r_2 \ \ \ \ \ 0\leq r_2<r_1, \\ r_1&=q_2r_2+r_3 \ \ \ \ \ 0\leq r_3<r_2, \\ &.\\ &.\\ &.\\ r_{n-2}&=q_{n-1}r_{n-1}+r_{n} \ \ \ \ \ 0\leq r_{n}<r_{n-1}, \\ r_{n-1}&=q_nr_{n}.\end{aligned}\] Notice that, we will have a remainder of \(0\) eventually since all the remainders are integers and every remainder in the next step is less than the remainder in the previous one. By Lemma 1.6.1, we see that \[\gcd(a,b)=\gcd(b,r_2)=\gcd(r_2,r_3)=\dots=\gcd(r_n,0)=r_n.\]

The full version of this theorem, with the \(s_j\)'s and \(t_j\), is called the **extended Euclidean Algorithm**, while a simpler version without those coefficients is know as **Euclidean Algorithm**.

The attentive reader will have seen that We did not actually prove that the \(s_j\)'s and \(t_j\)'s can be used, as claimed, to write the \(\gcd\) as a linear combination of \(a\) and \(b\). This proof is left as an exercise, below.

Example \(\PageIndex{1}\)

We will find the greatest common divisor of \(4147\) and \(10672\):
Note that \[\begin{aligned} 10672&=4147\cdot 2+2378,\\ 4147&=2378\cdot 1+1769,\\ 2378&=1769\cdot 1+609,\\ 1769&=609\cdot 2 +551,\\ 609&=551\cdot 1+58, \\ 551&=58\cdot 9+ 29,\\ 58&=29\cdot 2,\\\end{aligned}\] Hence \(\gcd(4147,10672)=29.\)

Exercise \(\PageIndex{1}\)

1. Use the Euclidean algorithm to find the greatest common divisor of \(412\) and \(32\) and express it in terms of the two integers.
2. Use the Euclidean algorithm to find the greatest common divisor of \(780\) and \(150\) and express it in terms of the two integers.
3. Find the greatest common divisor of \(70,98,108\).
4. Let \(a,b\in\NN\) be even. Prove that \(\gcd(a,b)=2\gcd(\dfrac{a}{2}, \dfrac{b}{2}).\)
5. Show that if \(a\in\NN\) is even and \(b\in\NN\) is odd, then \(\gcd(a,b)=\gcd(\dfrac{a}{2}, b)\).
6. Prove the *extended* part of the Extended Euclidean Algorithm.

UC Davis ChemWiki is licensed under a Creative Commons Attribution-Noncommercial-Share Alike 3.0 United States License.