

Abstract Algebra – Math 4010

Computing gcd and more

Preamble: For integers a and d , the expression “ d divides a ” means that $a/d \in \mathbb{Z}$ and assumes that $d \neq 0$. It is also written as $d|a$. Note that any non-zero integer divides 0. If $d \in \mathbb{Z}^*$ divides $a \in \mathbb{Z}$, then $\pm d$ divides $\pm a$. We may as well assume that $d \geq 1$ and that $a > 0$. If $a, b \in \mathbb{Z}^+$, then 1 divides both a and b , so the set of positive integers that divide a and b is never empty. If $d|a$ and $d|b$, then clearly $d \leq \min\{a, b\}$. Then defining $\gcd(a, b)$ to be the greatest integer that divides both a and b makes sense for $a, b \in \mathbb{Z}^+$.

Simple things: If $a|b$, then $\gcd(a, b) = a$. If p is a prime number and $1 \leq a < p$, then $\gcd(a, p) = 1$. When $\gcd(a, b) = 1$, we say that a and b are relatively prime.

Let $a, b \in \mathbb{Z}^+$ and suppose that $a \geq b$. Then a/b can always be written as $a/b = m + f$, where $m \in \mathbb{Z}^+$ and $f \in [0, 1) \cap \mathbb{Q}$. This representation is unique, and is equivalent to $a = mb + r$, where $r \in \mathbb{Z}$ and $0 \leq r < b$. Note that a positive integer d divides both a and b if and only if d divides both b and r . Note also that $r < b \leq a$.

To make the notation work out nicely, we rename a and b as a_0 and a_1 , and assume that $1 \leq a_1 \leq a_0$. We can now write

$$a_0 = m_1 a_1 + a_2,$$

where $0 \leq a_2 < a_1$. m_1 and a_2 are uniquely defined integers. We can define a sequence of numbers as follows. As long as $a_{k+1} > 0$, we can define m_{k+1} and a_{k+2} by dividing a_k by a_{k+1} and taking the remainder. That is,

$$a_k = m_{k+1} a_{k+1} + a_{k+2}.$$

Notice that the a_k sequence is strictly decreasing. For some $n \geq 1$, $a_{n+1} = 0$ and we can't go further. Then $a_n = \gcd(a_0, a_1)$. This is true because $\gcd(a_{k-1}, a_k) = \gcd(a_k, a_{k+1})$ for $1 \leq k \leq n$. The last pair is a_n and 0, with a greatest common divisor of a_n , as noted above. Also note that $n = 1$ if we start with a trivial case such as $a_1 = 1$ or $a_0 = a_1$, since the first remainder, a_2 , would be 0.

Now define a sequence of integers, b_k , for $0 \leq k \leq n + 1$ as follows. $b_{n+1} = 1$ and $b_n = 0$. For $1 \leq k \leq n$, let

$$b_{k-1} = b_k m_k + b_{k+1}.$$

It turns out that

$$a_k b_{k+1} - a_{k+1} b_k = \gcd(a_0, a_1),$$

for all $k \in \{0, 1, \dots, n\}$.

How can this be proved? The easiest way is to use 2×2 matrices to avoid messy calculations. Let $d = \gcd(a_0, a_1)$ let

$$\mathbf{D} = \begin{bmatrix} d & 0 \\ 0 & 1 \end{bmatrix}.$$

For $1 \leq k \leq n$, let

$$\mathbf{M}_k = \begin{bmatrix} m_k & 1 \\ 1 & 0 \end{bmatrix}.$$

Note that $\det \mathbf{D} = d$ and that $\det \mathbf{M}_k = -1, \forall k$. Finally, let

$$\mathbf{A}_k = \begin{bmatrix} a_k & b_k \\ a_{k+1} & b_{k+1} \end{bmatrix}$$

for $0 \leq k \leq n$. Note that $\mathbf{A}_n = \mathbf{D}$, and for $1 \leq k \leq n$, it is easy to compute

$$\begin{aligned} \mathbf{M}_k \mathbf{A}_k &= \begin{bmatrix} m_k & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} a_k & b_k \\ a_{k+1} & b_{k+1} \end{bmatrix} \\ &= \begin{bmatrix} m_k a_k + a_{k+1} & m_k b_k + b_{k+1} \\ a_k & b_k \end{bmatrix} \\ &= \begin{bmatrix} a_{k-1} & b_{k-1} \\ a_k & b_k \end{bmatrix} \\ &= \mathbf{A}_{k-1}. \end{aligned}$$

This means that

$$\begin{aligned} \mathbf{A}_0 &= \mathbf{M}_1 \mathbf{A}_1 \\ &= \mathbf{M}_1 \mathbf{M}_2 \mathbf{A}_2 \\ &= \mathbf{M}_1 \mathbf{M}_2 \mathbf{M}_3 \mathbf{A}_3 \\ &\vdots \\ &= \mathbf{M}_1 \mathbf{M}_2 \mathbf{M}_3 \dots \mathbf{M}_n \mathbf{A}_n \end{aligned}$$

giving

$$\begin{bmatrix} a_0 & b_0 \\ a_1 & b_1 \end{bmatrix} = \prod_{k=1}^n \mathbf{M}_k \mathbf{D}.$$

The above can also be written as

$$\begin{bmatrix} a_0/d & b_0 \\ a_1/d & b_1 \end{bmatrix} = \prod_{k=1}^n \mathbf{M}_k.$$

Also, $\det \mathbf{A}_0 = (-1)^n d$. Thus

$$a_0 b_1 - a_1 b_0 = (-1)^n d.$$

If n is even, $a_0 b_1 + a_1(-b_0) = d$ and if n is odd, $a_0(-b_1) + a_1 b_0 = d$.

The methods described above solve the problem of computing the greatest common divisor, d , of two positive integers and of expressing d as a “linear combination” of these two integers.

Example: Compute $\gcd(483, 399)$.

Solution:

$$\begin{array}{rcccccc} k & a_k & = & m_{k+1} & \star & a_{k+1} & + & a_{k+2} \\ 0 & 483 & = & 1 & \star & 399 & + & 84 \\ 1 & 399 & = & 4 & \star & 84 & + & 63 \\ 2 & 84 & = & 1 & \star & 63 & + & 21 \\ 3 & 63 & = & 3 & \star & 21 & + & 0 \end{array}$$

Thus, $n = 4$ and $\gcd(483, 399) = 21$, the last non-zero remainder.

$$\begin{aligned} \begin{bmatrix} a_0 & b_0 \\ a_1 & b_1 \end{bmatrix} &= \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 4 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 3 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 21 & 0 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 5 & 1 \\ 4 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 3 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 21 & 0 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 6 & 5 \\ 5 & 4 \end{bmatrix} \begin{bmatrix} 3 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 21 & 0 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 23 & 6 \\ 19 & 5 \end{bmatrix} \begin{bmatrix} 21 & 0 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 483 & 6 \\ 399 & 5 \end{bmatrix}. \end{aligned}$$

$$483 \times 5 - 399 \times 6 = 21.$$
