Sets of Common Divisors

Greatest common divisor

Given a natural number n, the set of its *divisors* is defined by set comprehension as follows

$$D(n) = \{ d \in \mathbb{N} : d \mid n \} \quad .$$

Example 53

1. $D(0) = \mathbb{N}$
2. $D(1224) = \left\{ \begin{array}{c} 1, 2, 3, 4, 6, 8, 9, 12, 17, 18, 24, 34, 36, 51, 68, \\ 72, 102, 136, 153, 204, 306, 408, 612, 1224 \end{array} \right\}$

Remark Sets of divisors are hard to compute. However, the computation of the greatest divisor is straightforward. :)

Going a step further, what about the *common divisors* of pairs of natural numbers? That is, the set

$$\mathrm{CD}(m, n) = \{\, d \in \mathbb{N} : d \mid m \wedge d \mid n \,\}$$

for $m, n \in \mathbb{N}$.

Example 54

$$\mathrm{CD}(1224, 660) = \{\, 1, 2, 3, 4, 6, 12 \,\}$$

Since $\mathrm{CD}(n, n) = \mathrm{D}(n)$, the computation of common divisors is as hard as that of divisors. But, what about the computation of the *greatest common divisor*?

Proposition For m and n natural numbers,

(1) $\underline{CD}(m,n) = \underline{CD}(n,m)$

(2) $\underline{CD}(m, n\cdot m) = \underline{D}(m)$

Corollary For a natural number ℓ,

(1) $\underline{CD}(\ell,\ell) = \underline{CD}(\ell,0) = \underline{D}(\ell)$

(2) $\underline{CD}(1,\ell) = \{1\}$

Proposition For m and n natural numbers,

(1) $\underline{CD}(m,n) = \underline{CD}(n,m)$

(2) $\underline{CD}(m, n \cdot m) = \underline{D}(m)$

PROOF: Let m and n be natural numbers.

(1) RTP $\underline{CD}(m,n) \overset{?}{=} \underline{CD}(n,m)$

$$\underline{CD}(m,n) = \{d \in \mathbb{N} : d \mid m \wedge d \mid n\}$$

$$\underline{CD}(n,m) = \{d \in \mathbb{N} : d \mid n \wedge d \mid m\}$$

Equivalently, for all $d \in \mathbb{N}$,

$$(d \mid m \wedge d \mid n) \iff (d \mid n \wedge d \mid m)$$

(2) $\underline{\text{RTP}}$ $\underline{CD}(m, n\cdot m) \overset{?}{=} \underline{D}(m)$

$$\underline{CD}(m, n\cdot m) = \{d \in \mathbb{N} \mid d \mid m \wedge d \mid n\cdot m\} \qquad \underline{D}(m) = \{d \in \mathbb{N} \mid d \mid m\}$$

Equivalently, for all $d \in \mathbb{N}$,

$$(d \mid m \wedge d \mid n\cdot m) \iff d \mid m.$$

$\boxtimes$

Lemma 56 (Key Lemma) *Let* m *and* m' *be natural numbers and let* n *be a positive integer such that* $m \equiv m' \pmod{n}$*. Then,*

$$\mathrm{CD}(m,n) = \mathrm{CD}(m',n) \ .$$

PROOF: Let m and m' be natural numbers and let n be a positive integer.

Assume: $m \equiv m' \pmod{n}$

RTP $\{d \in \mathbb{N} : d \mid m \wedge d \mid n\} \stackrel{?}{=} \{d \in \mathbb{N} : d \mid m' \wedge d \mid n\}$

Equivalently, for $d \in \mathbb{N}$,

$$(d \mid m \wedge d \mid n) \iff (d \mid m' \wedge d \mid n).$$

Lemma Let a, b, and c be integers. Then, c divides a and c divides b iff, and only if, c divides every integer linear combination of a and b.

PROOF: For arbitrary integers a, b, and c,

$$(c \mid a \wedge c \mid b) \iff \forall \text{ int. } i, j.\ c \mid i a + j \cdot b.$$

($\Rightarrow$) Assume $^{(1)} c \mid a$ and $^{(2)} c \mid b$.

Let i, j be arbitrary integers.

RTP: $c \mid ia + jb$

By (1), $a = ck$ for some integer k

By (2), $b = cl$ for some integer l.

Therefore, $ia + jb = c(ik + jl)$ and so

$c \mid ia + jb$ as required.

($\Leftarrow$) Assume $\forall i, j.\ c \mid ia + jb$.

Instantiating we have

$$c \mid 1 \cdot a + 0 \cdot b \quad \text{and} \quad c \mid 0 \cdot a + 1 \cdot b$$

Therefore

$$c \mid a \quad \text{and} \quad c \mid b$$

$\boxtimes$

Lemma 56 (Key Lemma) *Let* m *and* m' *be natural numbers and let* n *be a positive integer such that* $m \equiv m' \pmod{n}$*. Then,*

$$\mathrm{CD}(m, n) = \mathrm{CD}(m', n) \ .$$

PROOF: Let m and m' be natural numbers and let n be a positive integer.

<u>Assume</u>: $m \equiv m' \pmod{n}$

<u>RTP</u>: for all $d \in \mathbb{N}$,

$$(d \mid m \wedge d \mid n) \iff (d \mid m' \wedge d \mid n)$$

By assumption $m - m' = kn$ for some integer k. Therefore, m is an integer linear combination of m' and n, and m' is an integer linear combination of m and n.

NB: As an application of the key lemma, for a natural number m and a positive integer n, since $m \equiv \underline{\text{rem}}(m,n) \pmod n$ it follows that

$$\underline{CD}(m,n) = \underline{CD}(n, \underline{\text{rem}}(m,n))$$

Example:

$$\underline{CD}(34,13) = \underline{CD}(13,8) = \underline{CD}(8,5) = \underline{CD}(5,3)$$

$$= \underline{CD}(3,2) = \underline{CD}(2,1) = \underline{CD}(1,0)$$

$$= D(1) = \{1\}$$

Lemma 58 *For all positive integers* m *and* n,

$$\mathrm{CD}(\mathrm{m},\mathrm{n}) = \begin{cases} \mathrm{D}(\mathrm{n}) & \text{, \textit{if} } \mathrm{n} \mid \mathrm{m} \\ \mathrm{CD}\big(\mathrm{n}, \mathrm{rem}(\mathrm{m},\mathrm{n})\big) & \text{, \textit{otherwise}} \end{cases}$$

Lemma 58 *For all positive integers m and n,*

$$\mathrm{CD}(m,n) = \begin{cases} \mathrm{D}(n) & \text{, } \textit{if } n \mid m \\ \mathrm{CD}\big(n, \mathrm{rem}(m,n)\big) & \text{, } \textit{otherwise} \end{cases}$$

Since a positive integer n is the greatest divisor in $\mathrm{D}(n)$, the lemma suggests a recursive procedure:

$$\mathrm{gcd}(m,n) = \begin{cases} n & \text{, if } n \mid m \\ \mathrm{gcd}\,\big(n, \mathrm{rem}(m,n)\big) & \text{, otherwise} \end{cases}$$

for computing the *greatest common divisor*, of two positive integers m and n. This is

Euclid's Algorithm