Lec5A The Euclidean Algorithm

January 25, 2021 10:23 PM

Assignment #1 solutions posted tonight @ 11pm
Assignment #2 is posted.

An integral domain E is a Euclidean domain if

$\exists\ \nu : E \setminus \{0\} \longrightarrow \mathbb{N} \cup \{0\}$ satisfying

(i) $\nu(ab) \geq \nu(a) \qquad \forall a, b \in E \setminus \{0\}$

(ii) $\forall a, b \in E,\ b \neq 0 \quad \exists q, r \in E$ satisfying

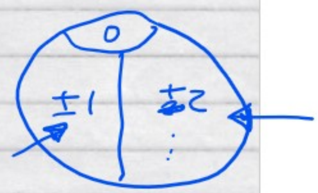
$$a = bq + r \quad \text{with} \quad r = 0 \text{ or } \nu(r) < \nu(b)$$

$a \div b.$

Properties of E

Let u be a unit in E and c, d be non-zero non-units in E

$\mathbb{Z}$



$\nu(a) = |a|.$

(iii) $\nu(u) = \nu(1)$

(iv) $\nu(c) > \nu(1)$

(v) $\nu(uc) = \nu(c)$

(vi) $\nu(cd) > \nu(c)$

(vii) $c \mid d$ and $d \mid c \Rightarrow \nu(c) = \nu(d)$

(viii) $\nu(d) > \nu(c) \Rightarrow d \nmid c$

The Euclidean Algorithm

The Euclidean Algorithm

Let E be a Euclidean domain with $\nu: E\setminus\{0\} \to \mathbb{N}\cup\{0\}$

Let $a,b \in E$, $b \neq 0$. Initialize $r_0 = a$ and $r_1 = b$.

$d|r_0 \quad d|r_1 \Rightarrow d|r_2$

$r_n|r_0$

$r_0 \div r_1 : \quad r_0 = q_2 r_1 + r_2 \qquad r_2 \neq 0 \quad \nu(r_2) < \nu(r_1)$

$r_n|r_1$

$r_1 \div r_2 : \quad r_1 = q_3 r_2 + r_3 \qquad r_3 \neq 0 \quad \nu(r_3) < \nu(r_2)$

$d|r_3$

$\vdots$

$r_n|r_{n-2} \qquad d|r_n$

$r_{n-2} \div r_{n-1} : \quad r_{n-2} = q_n r_{n-1} + r_n \qquad r_n \neq 0 \quad \nu(r_n) < \nu(r_{n-1})$

$r_{n-1} \div r_n : \quad \underline{r_{n-1}} = q_{n+1} \underline{r_n} + \underbrace{r_{n+1}}_{0} \qquad r_{n+1} = 0$

$r_n | r_{n-1}$

Claim r_n is a $\gcd(a,b)$.

Proof (i) Show $r_n|r_1 = b$ and $r_n|r_0 = a$ — r_n is a common divisor of r_0, r_1.

(ii) Show $d|r_0$ and $d|r_1 \Rightarrow d|r_n$

Claim n is finite (the algorithm terminates).

Proof $\nu(b) = \nu(r_1) > \nu(r_2) > \nu(r_3) > \cdots \geq 0$ — $\nu(u) = 0$

Therefore a $\gcd(a, b\neq 0)$ exists in E.

Theorem. Let $a,b \in E\setminus\{0\}$ where E is a Euc. dom. Then $\exists\, s,t \in E$ s.t.

$$sa + tb = g \quad \text{where } g = \gcd(a,b)$$

Proof (The extended Euclidean algorithm).

$r_0, r_1 \leftarrow a, b$ $\qquad$ $s_0, s_1 \leftarrow 1, 0$

$k \leftarrow 1$ $\qquad$ $t_0, t_1 \leftarrow 0, 1$

while $r_k \neq 0$ do

$\quad q_{k+1}, r_{k+1} \leftarrow \text{QUOREM}(r_{k-1} \div r_k)$ $\qquad$ $s_{k+1} \leftarrow s_{k-1} - q_{k+1} s_k$

$\quad \#\ r_{k-1} = r_k \cdot q_{k+1} + r_{k+1}$ $\qquad$ $t_{k+1} \leftarrow t_{k-1} - q_{k+1} \cdot t_k.$

$\quad k \leftarrow k+1.$

end while.

$n \leftarrow k-1$

output r_n, s_n, t_n.

a gcd(a,b).

Claim: $\underbrace{s_n}_{s} a + \underbrace{t_n}_{t} \cdot b = \underbrace{r_n}_{g}.$

Example: $a = 42$, $b = 26$ $\qquad$ $E = \mathbb{Z}$

$s_{k+1} = s_{k-1} - q_{k+1} \cdot s_k$

$t_{k+1} = t_{k-1} - q_{k+1} t_k.$

k	r_k	q_k	s_k	t_k
0	42	—	1	0
1	26	—	0	1 ←
2	16	1	$1-1\cdot 0=1$	$0-1\cdot 1=-1$
3	10	1	-1	1
4	6	1	2	-3
5	4	1	-3	5
6	2	1	5	-8
7	0	2	-13	21

$s_n a + t_n \cdot b = r_n$

$5 \cdot 42 - 8 \cdot 26 = 2$

$210 - 208$

Claim $s_k a + t_k \cdot b = r_k$ for $k = 0, 1, \dots, n, n+1.$

Proof (by double induction on k).

BASE $k=0$ $\qquad$ $\overset{1}{s_0} \cdot a + \overset{0}{t_0} b = \overset{a}{r_0}$ ✓

BASE $k=0$ $\quad \underset{1}{s_0} \cdot a + \underset{0}{t_0} b = \underset{a}{r_0}$ ✓

$k=1$ $\quad \underset{0}{s_1} a + \underset{1}{t_1} b = \underset{b}{r_1}$ ✓

$k>1$ STEP Assume (1) $s_{k-1} a + t_{k-1} b = r_{k-1}$

(2) $s_k a + t_k b = r_k$

To prove $\underline{s_{k+1} a + t_{k+1} b} = r_{k+1}$

$$s_{k+1} a + t_{k+1} b = (s_{k-1} - q_{k+1} s_k) a + (t_{k-1} - q_{k+1} t_k) \cdot b$$

$$= (s_{k-1} a + t_{k-1} \cdot b) - q_{k+1} (s_k a + t_k b)$$

QUOREM$(r_{k-1} \div r_k)$

$$= r_{k-1} - q_{k+1} \cdot r_k \quad \text{by the I. H.}$$

$r_{k-1} = r_k \cdot q_{k+1} + r_{k+1}$

$r_{k-1} - r_k \cdot q_{k+1} = r_{k+1}$

$$= r_{k+1}. \quad \text{(by Euc. division).}$$

Computing inverses in $\mathbb{Z}_m$. $\quad 3^{-1} \in \mathbb{Z}_{13}$.

Let $a \in \mathbb{Z}_m$ with $m > a > 0$.

1 Applying the EEA to input (m, a) we get $s, t, g \in \mathbb{Z}$ satisfying $s_n \cdot m + t_n \cdot a = g$ where $g = \gcd(a, b)$.

2 If $g > 1$ then output. "no inverse." $\quad a = 26 \; \mathbb{Z}_{42}$, $g = 2$

Otherwise $g = 1$.

mod m

$$0 + t_n \cdot a \equiv 1 \pmod{m} \Rightarrow t_n \text{ is the inverse of } a.$$

Notes. t_n can be $-$ve. How big can it be?

Can $|t| > m$?

Lemma: $|t_n| < \frac{m}{a}$ and $|s_n| < \frac{a}{g}$

Lemma: $|t_n| < \frac{m}{g}$ and $|s_n| < \frac{a}{g}$

$(g=1) \Rightarrow |t_n| < m \Rightarrow -m < t_n < m.$

③ If $t_n < 0$ then output $t_n + m$ else output t_n.

Note. We can save $\frac{1}{3}$ of the work by omitting computing the s_k's.