The Euclidean Algorithm

September 14, 2023 8:26 AM

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 $r_1 = b$.

$d|a \wedge d|b$ Show $d|r_n$

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

$d|r_2$

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

$d|r_3$

$\vdots \qquad \vdots$

$d|r_n$.

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

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

Claim r_n is a $\gcd(a,b)$.
Proof (i) Show $r_n | r_1 = b$ and $r_n | r_0 = a$
(ii) Show $d|r_0$ and $d|r_1 \Rightarrow d|r_n$
Claim n is finite (the algorithm terminates).
Proof $\nu(b) = \nu(r_1) > \nu(r_2) > \nu(r_3) > \cdots \geq 0$

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

Theorem Let E be a Euclidean domain and $a,b \in E \setminus \{0\}$. Then $\exists\, s,t \in E$ s.t.

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

Proof (the extended Euclidean algorithm).

Input $a, b \in E$.

Euc. Alg.

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

$k \leftarrow 1.$ $\qquad t_0, t_1 \leftarrow [0, 1.]$

while $r_k \neq 0$ do

$\quad q_{k+1} \leftarrow \text{Quo}(r_{k-1} \div r_k).$

$\quad r_{k+1} \leftarrow r_{k-1} - r_k q_{k+1}.$ —— $s_{k+1} \leftarrow s_{k-1} - s_k q_{k+1}$, $t_{k+1} \leftarrow t_{k-1} - t_k q_{k+1}.$

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

$\quad k \leftarrow k+1.$

end while

$n \leftarrow k-1.$

Output $\underset{\overset{\uparrow}{g}}{r_n}$ ——, $\underset{\overset{\uparrow}{s}}{s_n}, \underset{\overset{\uparrow}{t}}{t_n}$. $\qquad$ Claim $s_n a + t_n b = r_n$.

Example $a = 42,\ b = 26.$ $\mathbb{Z}.$

k	r_k	q_k	s_k	t_k
0	42		1	0
1	26		0	1
2	16	1	1	−1
3	10	1	−1	2
4	6	1	2	−3
5	4	1	−3	5

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

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

$s_n a + t_n b = r_n$

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

$\ \ \ 210 \quad - \quad 208$

	5	4	1	−3	5
$n=$	6	2	1	5	−8
	7	0	2	−13	21

g

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

Proof (double induction on k).

$k=0$ $\quad s_0 a + t_0 b = r_0$? $\quad 1\cdot a + 0 \cdot b = a$. ✓

$k=1$ $\quad s_1 a + t_1 b = r_1$? $\quad 0 \cdot a + 1 \cdot b = b$ ✓

$k>1$ Assume

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

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

Need to show $s_{k+1} a + t_{k+1} b = r_{k+1}$.

$$s_{k+1} a + t_{k+1} b \overset{\text{alg}}{=} (s_{k-1} - q_{k+1} s_k) a + (t_{k-1} - q_{k+1} t_k) b.$$

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

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

by alg.

$$= r_{k+1}.$$

Computing inverses in $\mathbb{Z}_m$.

Let $a \in \mathbb{Z}_m$ with $m > a > 0$. $\quad ?\, a^{-1}$

E.g. in $\mathbb{Z}_{13}$ $\quad 10^{-1} = 4$. $\quad 10 \cdot \boxed{4} \equiv 1 \mod 13$.

Applying the EEA(m,a) we get s, t s.t.

$$\hat{s} m + \hat{t} a = r_n = g.$$

If $g > 1$ then output "a is not invertible".

Otherwise

If $g > 1$ then output ...

Otherwise

$$0 + t_n a \equiv r_n = 1 \pmod{m}.$$

So t_n is "the inverse" but t_n can be -ve.

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

$\downarrow g = 1$

$|t_n| < m$ and $|s_n| < a$.

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

NB: We don't need to compute the s_k's.

This saves 1/3 of the work.