CLASS HANDOUT FOR THE EXTENDED EUCLIDEAN ALGORITHM

SAMUEL J. LOMONACO, JR.

The extended Euclidean algorithm is as follows:

Procedure EEA$(a_1, a_2; s_1, s_2)$

Given a_1 and a_2 in a Euclidean domain D, compute
$g = \gcd(a_1, a_2)$ and also compute $\overrightarrow{s} = (s_1, s_2) \in D \times D$
such that $g = s_1 a_1 + s_2 a_2$. We let $\overrightarrow{a}$ denote (a_1, a_2).
$c \longleftarrow |a_1|; \qquad \overrightarrow{c} = (1, 0);$
$d \longleftarrow |a_2|; \qquad \overrightarrow{d} = (0, 1);$
while $d \neq 0$ **do** {
$q \longleftarrow quo\,(c, d);$
$r \longleftarrow c - q \cdot d; \qquad \overrightarrow{r} \longleftarrow \overrightarrow{c} - q \cdot \overrightarrow{d};$
$c \longleftarrow d; \qquad \overrightarrow{c} \longleftarrow \overrightarrow{d};$
$d \longleftarrow r; \qquad \overrightarrow{d} \longleftarrow \overrightarrow{r};$ }
Normalize GCD
Please note that $u\,(\overrightarrow{a})$ denotes $(sign(a_1), sign\,(a_2))$, and $u(c)$ denotes $sign(c)$

$g \longleftarrow c$
$\overrightarrow{s} \longleftarrow \overrightarrow{c} \;/\; [\; u\,(\overrightarrow{a}) \cdot u(c)\;];$
return(g)
end

Example 1. *In the Euclidean domain $\mathbb{Z}$ if $a = 18$ and $b = 30$, then the sequence of values computed for $q, c, \overrightarrow{c}, d, \overrightarrow{d}$ in the above algorithm is as follows:*

Iteration No.	q	c	$\overrightarrow{c}$	d	$\overrightarrow{d}$
–	–	18	$(1,0)$	30	$(0,1)$
1	0	30	$(0,1)$	18	$(1,0)$
2	1	18	$(1,0)$	12	$(-1,1)$
3	1	12	$(-1,1)$	6	$(2,-1)$
r	2	6	$(2,-1)$	0	$(-5,3)$

Thus, $g = 6$, $s = 2$, and $t = -1$; i.e., $GCD\,(18, 30) = 6 = 2\,(18) - 1\,(30)$ as noted in the above example.

University of Maryland Baltimore County, Baltimore, MD 21250
E-mail address: lomonaco@umbc.edu

Date: April 8, 2007.