CLASS HANDOUT FOR THE EXTENDED EUCLIDEAN ALGORITHM

SAMUEL J. LOMONACO, JR.

1. Extended Euclidean Alghorithm

The extended Euclidean algorithm is as follows:

Procedure EEA$(a, b; s, t)$

Given a and $b$in a Euclidean domain D, compute
$g = \gcd(a, b)$ and also compute elements $s, t \in D$
such that $g = sa + tb$.
$c \longleftarrow |a|; \qquad d \longleftarrow |b|$
$c_1 \longleftarrow 1; \qquad d_1 \longleftarrow 0$
$c_2 \longleftarrow 0; \qquad d_2 \longleftarrow 1$
while $d \neq 0$ **do** {
$q \longleftarrow quo\,(c, d); \qquad r \longleftarrow c - q \cdot d$
$r_1 \longleftarrow c_1 - q \cdot d_1; \qquad r_2 \longleftarrow c_2 - q \cdot d_2$
$c \longleftarrow d; \qquad c_1 \longleftarrow d_1; \qquad c_2 \longleftarrow d_2$
$d \longleftarrow r; \qquad d_1 \longleftarrow r_1; \qquad d_2 \longleftarrow r_2 \quad \}$
Normalize GCD
$g \longleftarrow c$
$s \longleftarrow c_1 / (u(a) \cdot u(c)); \qquad t \longleftarrow c_2 / (u(b) \cdot u(c))$
return(g)
end

Example 1. *In the Euclidean domain Z if $a = 18$ and $b = 30$, then the sequence of values computed for $q, c, c_1, c_2, d, d_1, d_2$ in the above algorithm is as follows:*

Iteration No.	q	c	c_1	c_2	d	d_1	d_2
–	–	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: February 8, 2006.