CLASS HANDOUT FOR THE EXTENDED EUCLIDEAN ALGORITHM

SAMUEL J. LOMONACO, JR.

The extended Euclidean algorithm is as follows:

Procedure Euclid-Extended(α, β)
local a, b, B, r, q
global A
\# Input is integers α and β, not both zero.
\# Final value of $a = \gcd(\alpha, \beta)$ and final value of $A = (x, y) \in \mathbb{Z} \times \mathbb{Z}$
\# is such that $\gcd(\alpha, \beta) = \alpha x + \beta y$. Moreover, the final value A is
\# a side effect of the algorithm
$a \longleftarrow |\alpha|; \qquad A = (1, 0)$
$b \longleftarrow |\beta|; \qquad B = (0, 1)$
while $b \neq 0$ **do**
$q \longleftarrow \left\lfloor \frac{a}{b} \right\rfloor$
$r \longleftarrow a - q \cdot b; \qquad R \longleftarrow A - q \cdot B$
$a \longleftarrow b; \qquad A \longleftarrow B$
$b \longleftarrow r; \qquad B \longleftarrow R$
end while;
return(a)
end

Example 1. *Let* $\alpha = 18$ *and* $\beta = 30$. *Then the sequence of values computed for* q, a, A, b, B *in the above algorithm is as follows:*

Iteration No.	q	a	A	b	B
–	–	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	$(2, -1)$
4	2	6	$(2, -1)$	0	–

Thus, $\gcd(18, 30) = 6 = 2 \cdot (18) + (-1) \cdot (30)$.

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

Date: November 23, 2010.