Lab4: Euclidean Algorithm.

Manuel Lecha.

Proof the following properties of the gcd for 2 given integers a, b

a) $gcd(2a,2b) = 2gcd(a,b)$

b) $gcd(2a+1,2b) = gcd(2a+1,b)$

c) $gcd(2a+1,2b+1) = gcd(min(2a+1,2b+1), |a-b|)$

Recall that an integer d is said to be the $gcd(a,b)$ for two given integers a,b if and only if $d|a$ $d|b$ and for every r such that $r|a$ and $r|b$, $r|d$.

a) In fact this property is true for every positive integer m.

$$gcd(ma,mb) = m\,gcd(a,b)$$

We know that if $d = gcd(a,b)$, then $d|a$, $d|b$ and by Bezout identity, there exist s and t integers such that $sa+tb = d$. One can note that everything holds if and only if $dm|am$, $dm|bm$ and $sam+tbm = dm$.

b) If $d = gcd(2a+1,2b)$, then $d|2a+1$ and $d|b$. However if $d|2a+1 \Rightarrow d \neq 2$ and therefore $d|2b$ if and only if $d|b$. Thus $gcd(2a+1,2b) = gcd(2a+1,b)$.

c) Suppose $2a+1 \leq 2b+1$. Then, $gcd(2a+1,2b+1) = gcd(2a+1, gcd(2a+1,2b+1)) =$ $gcd(min\{2a+1,2b+1\}, gcd(2a+1,2b+1))$. If $d = gcd(2a+1,2b+1)$ iff $d|2a+1$ and $d|2b+1$ iff $d \neq 2$ and $d| |2a+1-(2b+1)|$ iff $d||2(a-b)|$ iff $d||a-b|$ so $gcd(min\{2a+1,2b+1\}, gcd(2a+1,2b+1)) = gcd(min\{2a+1,2b+1\}, |a-b|)$.