Paradigm: Tail Recursion

GCD: Euclid's Algorithm

R. Inkulu
http://www.iitg.ac.in/rinkulu/

Definition

The *greatest common divisor (gcd)* of two positive integers a and b, $gcd(a, b)$, is the largest integer that divides both a and b.

w.l.o.g., assume $a > b \geq 0$.

ex. $gcd(30, 21) = 3$

GCD recursion Theorem

$gcd(a, b) = gcd(b, a\ mod\ b)$

The Euclid's Algorithm

Let $r_0 = a$ and $r_1 = b$. If the division algorithm is successively applied to obtain $r_j = r_{j+1}q_{j+1} + r_{j+2}$, with $0 < r_{j+2} < r_{j+1}$ for $j = 0, 1, 2, \ldots, k-2$ and $r_{k+1} = 0$, then $gcd(a, b) = r_k$, the last nonzero remainder.

note that $q_1, q_2, \ldots, q_{k-1} \geq 1$, $q_k \geq 2$, and $r_k \geq 1$.

```
Euclid-GCD(a, b)
    if b == 0 return a
    else return Euclid-GCD(b, a mod b)
```

Correctness

- from the GCD recusion Theorem, $gcd(r_0, r_1) = gcd(r_1, r_2) = \ldots = gcd(r_{k-1}, r_k) = gcd(r_k, r_{k+1} = 0) = r_k$; and,
- $r_0 > r_1 \ldots > r_k > r_{k+1} = 0$; in other words, the algorithm is guaranteed to be terminated.

Analysis: Lame's Theorem

The number of recursive calls made to find the $gcd(a, b)$ using the Euclidean algorithm is $O(\lg b)$. $\leftarrow$ weakly-polynomial time algorithm

- If $gcd(a, b)$ performs k recursive calls, then $a \geq f_{k+2}$ and $b \geq f_{k+1}$.

  proof by induction on k

- The k^{th} Fibonacci number equals to $\frac{\alpha^k - \beta^k}{\sqrt{5}}$, where $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$.

One more interesting observation

- The $gcd(a,b)$ is the least positive element of the set $\{ax + by : x, y \in Z\}$ i.e., if $d \mid a$ and $d \mid b$, then $d \mid gcd(a,b)$.