DAC algorithms and Recursion

Balaji Raghavachari
rbk@utdallas.edu

Computing x^n

Naive algorithm for computing x^n (RT: $O(n)$):

naivePower(x, n, p) // Return $x^n mod p$
$prod \leftarrow 1$
for $i \leftarrow 1$ **to** n **do**
    $prod \leftarrow (prod * x)\%p$
return $prod$

DAC algorithm

Power(x, n, p) // RT: $O(\log n)$
if $n = 0$ **then**
    return 1
else if $n = 1$ **then**
    return x
else
    $half \leftarrow$ Power($x, n/2, p$)
    $res \leftarrow (half * half)\%p$
    if $n\%2 = 0$ **then**
        return res
    else
        return $(res * x)\%p$

Alternate DAC algorithm

Power(x, n, p) // RT: $O(\log n)$
if $n = 0$ **then**
    return 1
else if $n = 1$ **then**
    return x
else
    $res \leftarrow$ Power($(x * x)\%p, n/2, p$)
    if $n\%2 = 0$ **then**
        return res
    else
        return $(res * x)\%p$