Transform and Conquer

$$p(x) = 2x^4 - x^3 + 3x^2 + x - 5$$

Horner's rule for evaluating a polynomial

$$p(x) = x(2x^3 - x^2 + 3x + 1) - 5$$
$$= x(x(2x^2 - x + 3) + 1) - 5$$
$$= x(x(x(2x - 1) + 3) + 1) - 5$$

```
Horner(P[0..n], x)
// Evaluates a polynomial at a
// given input by Horner's rule.
// Input: An array P[0..n] of
// coefficients of a polynomial of
// degree n, stored from the lowest
// to the highest, and a number x.
// Output: The value of the
// polynomial at x.
  p ← P[n]
  for i ← n-1 downto 0 do
     p ← x * p + P[i]
  return p
```

$P = [-5, 1, 3, -1, \overset{n}{2}]$

x	p	n	i
3	2	4	
	5		3
	18		2
	55		1
	160		0

$x - 3 \,\overline{)\, 2x^4 - x^3 + 3x^2 + x - 5}$

$$\begin{array}{r|rrrrr} 3 & 2 & -1 & 3 & 1 & -5 \\ & \downarrow & 6 & 15 & 54 & 165 \\ \hline & 2 & 5 & 18 & 55 & 160 \end{array}$$

divisor $x - x_0 = x - 3$

quotient $2x^3 + 5x^2 + 18x + 55$

remainder 160

Binary Exponentiation

Computing a^n

Let $n = b_I \ldots b_i \ldots b_0$

$p(x) = b_I x^I + \ldots + b_i x^i + \ldots + b_0$, where $x = 2$

$13 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$

Example: a^{13}

$n = 13$, binary 1101

$a^n = a^{p(2)} = a^{b_I 2^I + \ldots + b_i 2^i + \ldots + b_0}$

Horner's rule for the binary polynomial $p(2)$	Implications for $a^n = a^{p(2)}$
$p \leftarrow 1$	$a^p \leftarrow a^1$
for $i \leftarrow I-1$ downto 0 do	for $i \leftarrow I-1$ downto 0 do
$p \leftarrow 2p + b_i$	$a^p \leftarrow a^{2p+b_i}$

But a^{2p+b_i}

$$= a^{2p} \cdot a^{b_i}$$
$$= (a^p)^2 \cdot a^{b_i} = \begin{cases} (a^p)^2 & \text{if } b_i = 0 \\ (a^p)^2 \cdot a & \text{if } b_i = 1 \end{cases}$$

```
LeftRightBinaryExponentiation(a, b(n))
  // Computes a^n
  // Input: a number 'a' and a list
  // b(n) of binary digits b_I, ..., b_0
  product ← a
  for i ← I-1 downto 0 do
     product ← product * product
     if b_i = 1:
        product ← product * a
  return product
```

$2^{13} \Rightarrow a = 2$, $b(n) = 1101$

product	a	i
~~2~~	2	~~2~~
~~4~~		1
~~8~~		0
~~64~~		
~~4096~~		
8192		

Number of multiplications $M(n)$:

$$b - 1 \le M(n) \le 2(b-1)$$

where b is the number of bits used to represent exponent n

leading 1, rest all 0s => power of 2

all 1s => power of 2 − 1

$b - 1 = \lfloor \lg n \rfloor = \Theta(\lg n)$