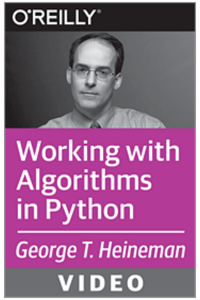
O'REILLY®

Mathematical Algorithms



Optimizing Mathematical Computations

- Mathematical algorithms can noticeably improve number crunching performance
  - I will show you one such example
  - Numerical Recipes (www.nr.com) offers complete solutions so you can avoid writing your own

Surprising Optimizations

- Consider computing $x^n = x * x * \dots * x$
  - Can you produce same computation with fewer than $n - 1$ multiplications?
  - Consider $x^6 = (x * x * x)^2$ which uses only 3!
- Identify algorithm to produce minimal for all *n*
  - ExponentiationBySquaring
  - Surprisingly versatile algorithm

Demonstrate Small Example

Let's compute 2^{13} as follows

$$
\begin{aligned}
2^{13} &= 2 * (2*2)^6 = 2 * 4^6 \\
&= 2 * (4*4)^3 = 2 * 16^3 \\
&= 2 * 16 * (16*16)^1 \\
&= 2 * 16 * 256 = 8192
\end{aligned}
$$

5 multiplications in total

Identifying proper sub-problems is key to this algorithm

Algorithm Pseudocode

Reduce problem in half with each recursive call

EXPONENTIATIONBYSQUARING		
Best case	Average case	Worst case
O(*log n*)	O(*log n*)	O(*log n*)

```
def exponent(x, n):
  if n == 0: return 1
  if n == 1: return x
  if n % 2:
    return x * exponent(x*x, ⌊n/2⌋ )
return exponent (x*x, n/2)
```

$$2^{13} = 2 * (2*2)^6$$

$$4^6 = (4*4)^3$$

Matrix Exponentiation

- Matrices are two-dimensional structures
  - When a matrix is squared, it can be raised to the n^{th} degree
  - Here matrix $\begin{vmatrix} 1 & 1 & 1 \\ 2 & 1 & 2 \\ 1 & 2 & 1 \end{vmatrix}$ is squared to produce another matrix

$$\begin{vmatrix} 1 & 1 & 1 \\ 2 & 1 & 2 \\ 1 & 2 & 1 \end{vmatrix} \times \begin{vmatrix} 1 & 1 & 1 \\ 2 & 1 & 2 \\ 1 & 2 & 1 \end{vmatrix} = \begin{vmatrix} 4 & 4 & 4 \\ 6 & 7 & 6 \\ 6 & 5 & 6 \end{vmatrix}$$

- Same approach works
  - Let's review in code

Mathematical Problem

622288097498926496141095869268883999563096063592498055290461

- Is a given number prime?
- Costly prime factorization proves exact answer
  - Fermat’s little theorem suggests probabilistic probe
  - if p is a prime number, then for any integer a, the number $a^p - a$ is an integer multiple of p
  - In other words, $a^p = a \text{ modulo } p$ or $a^{p-1} = 1 \text{ modulo } p$
- An estimate which can be run multiple times