

COSC229 Tutorial No. 5 Seminumerical Algorithms

(1) Obtain the addition and multiplication tables for Z_7 . Perform $5+6$ and $5*6$ in the table.

(2) Compute the 9-th Fibonacci number $x(9)$ by the direct formula

$$\begin{aligned}x(0) &= 0, \quad x(1) = 1, \\x(n) &= x(n-1) + x(n-2) \text{ for } n \geq 2,\end{aligned}$$

and by repeated squaring of a matrix.

(3) Trace Euclid's algorithm with $a = 25$ and $b = 7$. Obtain $25^{-1} \bmod 7$ and $7^{-1} \bmod 25$ from the trace.

(4) Erathostenes sieve method for generating prime numbers not greater than n is described informally as follows.

Sieve out all multiples of 2 between 3 and n .

Sieve out all multiples of 3 between 4 and n .

...

Sieve out all multiples of i between $i+1$ and n .

...

The array a holds 0 or 1 indicating i is non-prime if $a[i]=1$. All are initialized to 0. In the above process, sieving is done by setting the array elements to 1. Thus

After sieving by 2, $a = (0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$
 1 2 3 4 5 6 7 8 9 10

After sieving by 3, $a = (0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$
 1 2 3 4 5 6 7 8 9 10

In the above i can be odd numbers apart from the initial 2.

(A) Prove that the above i can be less than the square root of n .

(B) Write a program for this method to list up all prime numbers up to n .

(C) Prove that the time for this algorithm is $O(n \log n)$. Note that this time is not a polynomial of the bit length of n , that is, $\log n$.