

COSC229 Tutorial No.5 Seminumerical Algorithms – Solutions

Prepared by Sharon Duan (ddd12)

(1) Z_7

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$$5 + 6 = 4 \text{ in } Z_7$$

*	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

$$5 * 6 = 2 \text{ in } Z_7$$

(2) Calculate the 9th Fibonacci number

By direct formula:

$$x(0) = 0, x(1) = 1, x(n) = x(n-1) + x(n-2) \text{ for } n \geq 2$$

$x(0)$	$x(1)$	$x(2)$	$x(3)$	$x(4)$	$x(5)$	$x(6)$	$x(7)$	$x(8)$	$x(9)$
0	1	1	2	3	5	8	13	21	34

By repeated squaring:

We need to calculate $(x(8) \ x(9)) = (x(0) \ x(1)) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^8$ (see P.70 for the formula)

To calculate $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^8$, we use repeated squaring:

The first step is to convert 8 into binary number: $8 = (1000)_b$

Trace the algorithm:

$$y=1, x = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

$$i=3, y=y*y=1, b(3)=1, y=y*x = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \quad (\text{Note: } b(n) \text{ is the binary number})$$

$$i=2, y=y*y = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0+1 & 0+1 \\ 0+1 & 1+1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}, b(2)=0$$

$$i=1, y=y*y = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 1+1 & 1+2 \\ 1+2 & 1+4 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}, b(1)=0$$

$$i=0, y=y*y = \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix} = \begin{bmatrix} 4+9 & 6+15 \\ 6+15 & 9+25 \end{bmatrix} = \begin{bmatrix} 13 & 21 \\ 21 & 34 \end{bmatrix}$$

$$\text{Finally: } (x(8) \ x(9)) = (0 \ 1) \begin{bmatrix} 13 & 21 \\ 21 & 34 \end{bmatrix} = (0+21 \ 0+34) = (21 \ 34)$$

(3) Trace Euclid's algorithm with $a=25$ and $b=7$:

$$25 = 7*3 + 4, q(1) = 3, r(2) = 4$$

$$7 = 4*1 + 3, q(2) = 1, r(3) = 3$$

$$4 = 3*1 + 1, q(3) = 1, r(4) = 1$$

$$3 = 1*3 + 0, q(4) = 3, r(5) = 0$$

$\gcd(25, 7) = r(4) = 1 \Rightarrow 25$ and 7 are mutually prim.

Tracing the sequences $a(i)$ and $b(i)$:

$$a(2) = a(0) - q(1)a(1) = 0 - 3 = -3$$

$$b(2) = b(0) - q(1)b(1) = 1 - 0 = 1$$

$$a(3) = a(1) - q(2)a(2) = 1 - 1(-3) = 4$$

$$b(3) = b(1) - q(2)b(2) = 0 - 1*1 = -1$$

$$a(4) = a(2) - q(3)a(3) = -3 - 1*4 = -7$$

$$b(4) = b(2) - q(3)b(3) = 1 - 1*(-1) = 2$$

$$\text{We obtain } 25*b(4) + 7*a(4) = 25*2 + 7*(-7) = 1 \Rightarrow 2a - 7b = 1$$

If we perform mod 7 on both sides of the equation, we will have $25*2 = 1 \pmod{7}$

That means 2 is the inverse of 25 when mod 7, so $25^{-1} = 2 \pmod{7}$

Similarly, if we perform mod 25 on both sides, we will have $7*(-7) = 1 \pmod{25}$

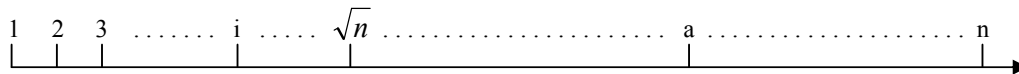
That means $7^{-1} = -7 \pmod{25}$

To get a positive number, we add 25 to the RHS and obtain $7^{-1} = 18 \pmod{25}$

So the inverse of 7 when mod 25 is 18

(4) Erathostenes sieve method

(A) Each time when we want to sieve by a number i , we actually want to sieve out all multiples of i from $i+1$ to n , which can be represented as $a * i = b$, ($i + 1 \leq b \leq n$). Since the maximum value of b is n , one of its divisors (a or i in the equation above) must be smaller than or equal to \sqrt{n} , and another one must be greater than or equal to \sqrt{n} . Therefore, when a is greater than \sqrt{n} , i must be less than \sqrt{n} . Please see the number line below:



(C) When we sieve by 2, we sieve out every second number, so totally we sieve $n/2$ times. Similarly, when we sieve by 3, we sieve $n/3$ times... Carry on with this, and we finally sieve by \sqrt{n} , then we sieve n/\sqrt{n} times. Therefore the total times we perform sieving should be:

$$\frac{n}{2} + \frac{n}{3} + \dots + \frac{n}{\sqrt{n}} = n\left(\frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{\sqrt{n}}\right)$$

Since $\left(\frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{\sqrt{n}}\right) = O(\log n)$, altogether it takes $O(n \log n)$ time.