

CS/MATH 111, Discrete Structures - Fall 2018.

Discussion 10 - Review

Andres, Sara, Elena

University of California, Riverside

December 6, 2018

Outline

Problem 1

Problem 2

Problem 3

Problem 4

Problem 5

Problem 6

Problem 1

- For pseudo-code below, tell what is the number of words printed if the input is n . Give a recurrence and then its solution (use Θ notation).

Pseudo-code	Recurrence and solution
<pre>Procedure Geez(n) if n>1 then print("geeze") print("geeze") Geez(2n/3)</pre>	

Master theorem

Theorem

Let $a \geq 0$, $b > 0$, $c > 0$ and $d \geq 0$. If $T(n)$ satisfies the recurrence then

$$T(n) = a \cdot T\left(\frac{n}{b}\right) + c \cdot n^d$$

$$T(n) = \begin{cases} \Theta(n^{\log_b a}) & a > b^d \\ \Theta(n^d \log n) & a = b^d \\ \Theta(n^d) & a < b^d \end{cases}$$

Problem 1

- ▶ Solution: $T(n) = T(2n/3) + 2$

$$a = 1, b = \frac{3}{2}, c = 2, d = 0$$

$$\text{Case 2: } n^0 \cdot \log(n) = \log(n)$$

- ▶ Other examples:

<http://people.csail.mit.edu/thies/6.046-web/master.pdf>

Outline

Problem 1

Problem 2

Problem 3

Problem 4

Problem 5

Problem 6

Problem 2

- ▶ For any integer $x > 4$, it is not possible that all three numbers x , $x + 2$ and $x + 4$ are prime.

Problem 2

► Solution:

- Since x is greater than 4 it cannot be divisible by 3. So, x is either in the form of $3q + 1$ or $3q + 2$.
- If $x = 3q + 1$ then:

$$x + 2 = 3q + 1 + 2 = 3q + 3 = 3(q + 1) = 3q'$$

hence $x + 2$ is divisible by 3. Therefore, it is not a prime number.

- If $x = 3q + 2$ then:

$$x + 4 = 3q + 2 + 4 = 3q + 6 = 3(q + 2) = 3q'$$

hence $x + 4$ is divisible by 3. Therefore, it is not a prime number.

Outline

Problem 1

Problem 2

Problem 3

Problem 4

Problem 5

Problem 6

Problem 3

- ▶ Prove that $1 + 3 + 5 + \dots + (2n - 1) = n^2$ for any integer $n \geq 1$. (The expression on the left-hand-side is the sum of the first n odd natural numbers). You can use mathematical induction or any other proof method.

Problem 3

► Solution:

► Base case:

$$1 = 1^2$$

► Assumption:

$$1 + 3 + 5 + \cdots + (2k - 1) = k^2$$

► Induction:

$$1 + 3 + 5 + \cdots + (2(k + 1) - 1) = (k + 1)^2$$

$$1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = (k + 1)^2$$

$$k^2 + (2k + 1) = (k + 1)^2$$

$$k^2 + 2k + 1 = k^2 + 2k + 1$$

Outline

Problem 1

Problem 2

Problem 3

Problem 4

Problem 5

Problem 6

Problem 4

- ▶ Explain how the RSA cryptosystem works

Problem 4

► Solution:

Initialization	<p>Choose two different primes p and q, and let $n=pq$. Let $\phi(n) = (p-1)(q-1)$.</p> <p>Choose an integer e relatively prime to $\phi(n)$.</p> <p>Let $d=e^{-1}(\text{mod } \phi(n))$.</p> <p>Public key is $P=(n,e)$ and Secret key is $S=d$.</p>
Encryption	<p>If M is the message then its encryption is</p> $E(M) = M^e \text{ rem } n$
Decryption	<p>If C is the ciphertext then it is decrypted as</p> $D(C) = C^d \text{ rem } n$

Problem 4

- Below you are given five choices of parameters p, q, e, d of RSA. For each choice tell whether these parameters are correct. If not, give a brief justification.

p	q	e	d	correct	Justify if not correct
23	51	18	89		
23	11	33	103		
3	7	5	5		
17	17	3	171		
17	11	13	37		

Problem 4

► Solution:

p	q	e	d	correct	Justify if not correct
23	51	18	89	NO	51 is not prime
23	11	33	103	NO	33 is not relatively prime to $\phi(n)$
3	7	5	5	YES	
17	17	3	171	NO	p and q should be different
17	11	13	37	YES	

Outline

Problem 1

Problem 2

Problem 3

Problem 4

Problem 5

Problem 6

Problem 5

- ▶ Use Fermat's Little theorem to compute the following values:
 - ▶ $78^{112} \pmod{113}$
 - ▶ $3^{39635} \pmod{31}$

Problem 5

- ▶ Use Fermat's Little theorem¹ to compute the following values:
 - ▶ $78^{112} \pmod{113} \equiv 1 \pmod{113}$
 - ▶ $3^{39635} \pmod{31} = 3^{30 \cdot 1321 + 5} \pmod{31} = (3^{30})^{1321} \times 3^5 \pmod{31}$

$$\begin{aligned} &\equiv (1)^{1321} \times 3^5 \pmod{31} \\ &\equiv 243 \pmod{31} \\ &\equiv 26 \pmod{31} \end{aligned}$$

¹ $a^{p-1} \equiv 1 \pmod{p}$

Outline

Problem 1

Problem 2

Problem 3

Problem 4

Problem 5

Problem 6

Problem 6

- ▶ Kevin is planning a 32-day trip to Scandinavia. He wants to spend at least 3 days in Finland, then between 7 and 14 days in Sweden, and later between 6 and 11 days in Norway. Compute the number of possible itineraries for his trip.

Problem 5

- ▶ Dealing with lower and upper bounds:

- ▶ $7 \leq S \leq 14, S' = S - 7:$

$$0 \leq S' \leq 7$$

- ▶ $6 \leq N \leq 11, N' = N - 6:$

$$0 \leq N' \leq 5$$

- ▶ $3 \leq F \implies 3 \leq F \leq 32 - 7 - 6 \implies 3 \leq F \leq 19, F' = F - 3:$

$$0 \leq F' \leq 16$$

- ▶ Stating new number of solutions from new bounds:

- ▶ $S + N + F = 32 \implies$

- ▶ $S' + 7 + N' + 6 + F' + 3 = 32 \implies$

- ▶ $S' + N' + F' = 16$

Problem 5

- Finding $\mathbf{S}(S' \leq 7 \cap N' \leq 5 \cap F' \geq 17)$ using Inclusion-Exclusion principle:

► $\mathbf{S} = S_{total} - S(S' \geq 8 \cup N' \geq 6 \cup F' \geq 17)$

► $\mathbf{S} = S_{total} - [S(S' \geq 8) + S(N' \geq 6) + S(F' \geq 17) - S(S' \geq 8 \cap N' \geq 6) - S(S' \geq 8 \cap F' \geq 17) - S(N' \geq 6 \cap F' \geq 17) + S(S' \geq 8 \cap N' \geq 6 \cap F' \geq 17)]$

► $\mathbf{S} = \binom{16+3-1}{3-1} - [\binom{16-8+3-1}{3-1} + \binom{16-6+3-1}{3-1} + \binom{16-17+3-1}{3-1} - \binom{16-14+3-1}{3-1} - \binom{16-25+3-1}{3-1} - \binom{16-23+3-1}{3-1} + \binom{16-31+3-1}{3-1}]$

► $\mathbf{S} = \binom{18}{2} - [\binom{10}{2} + \binom{12}{2} + \binom{1}{2} - \binom{4}{2} - \binom{-7}{2} - \binom{-5}{2} + \binom{-13}{2}]$

► $\mathbf{S} = \binom{18}{2} - [\binom{10}{2} + \binom{12}{2} + 0 - \binom{4}{2} - 0 - 0 + 0]$