DISCRETE MATH 37181 HOMEWORK SHEET 10

INSTRUCTIONS. Try these sometime after your tutorial and before the next lecture. Set aside some time each week to keep up with the homework. Partial solutions at the end of the PDF.

1. The number of edges in a graph with degree sequence $2, 2, 2, 3, 3, 4, 4$ is

   A. 8 **C**. 9 **E**. no graph exists with this degree sequence.

   B. 10 **D**. 11

2. Let G be the undirected graph with adjacency matrix

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

   The number of paths of length 4 from any vertex of G to itself is

   A. 8 **C**. 4 **E**. the answer is different depending on which vertex is chosen.

   B. 6 **D**. 2

3. Use the Euclidean algorithm (backwards) to find the multiplicative inverse of $29 \mod 240$.

4. Suppose that Bob enciphers m by calculating $c = m^{29} \mod 287$. How does Alice find m? [1]

5. Using the copy of the 2018 final exam provided on Canvas try questions 1-10 and 16, 17, 18, 21, 22, 24, 25, 26, 27.

END OF HOMEWORK SHEET 10

Date: Week 10.

[1] Hint: This question is asking: Alice set up her RSA with $e = 29$ and $n = 287$. So:
(a) Find the prime factorization of 287.
(b) Find $\varphi(287)$.
(c) Now find d so that Alice can decipher.

Brief solutions:

1. B

2. B

   The graph is a triangle. The number of paths should be the same no matter which vertex. (Next week we will learn a cool method to calculate the number of paths between any two points in any finite graph.)

3. $$\begin{aligned} 240 &= 8 \times 29 + 8 \\ 29 &= 3 \times 8 + 5 \\ 8 &= 1 \times 5 + 3 \\ 5 &= 1 \times 3 + 2 \\ 3 &= 1 \times 2 + 1 \end{aligned}$$

   so

   $$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (5 - 3) \\ &= 2.3 - 5 \\ &= 2(8 - 5) - 5 \\ &= 2.8 - 3.5 \\ &= 2.8 - 3(29 - 3.8) \\ &= 11.8 - 3.29 \\ &= 11(240 - 8.29) - 3.29 \\ &= 11.240 - 91.29 \end{aligned}$$

   so $-91 \equiv 149$ is the inverse required.
   Check: $149.29 = 4321 = 4320 + 1 = 18.240 + 1$

4. Alice set up her RSA with $e = 29$ and $pq = 287$. Prime factorization:

   $$287 = 41.7$$

   $$\phi(287) = (41 - 1)(7 - 1) = 40.6 = 240$$

   By the previous question we have $29.149 \equiv 1 \mod 240$ so we need $d = 149$.

   Answer: Alice finds m by computing $[c^{149}]_{287}$.