DISCRETE MATH 37181 TUTORIAL WORKSHEET 10

INSTRUCTIONS. Complete these problems in groups of 3-4 at the whiteboard. Partial solutions at the end of the PDF. Aim to spend around 40 minutes on RSA and 40 minutes on graph questions.

1. Alice constructs an RSA system by choosing $n = 55$ and $e = 17$.
   (a) Find $\varphi(55)$.
   (b) Find d.
   (c) Bob wants to send Alice the message $m = 27$. Compute his encoded message c.
   (d) Alice receives c from Bob (as you computed in part (b)). Perform the steps to decode it to get m [1].

2. Alice constructs an RSA system by choosing $n = 143$ and $e = 13$. Bob sends $c = 4$ to Alice. What was Bob's intended message?

3. (From LPC 2021) [2]
   (a) Alice constructs an RSA system by choosing $n = 1271$ and $e = 131$. Find d. Show all steps.
   (b) Bob sends a message encoded as $c = 11$ to Alice. What was his message m? Show all steps.

4. Write down the definition of the following.
   (a) degree of a vertex
   (b) simple path
   (c) adjacency matrix for a graph

5. (a) Consider the degree sequence $3, 3, 2, 2, 1, 1, 1$. Draw as many different graphs with this degree sequence as you can. [3]

   (b) Consider the degree sequence $4, 1, 1, 1, 1$. Draw as many different graphs with this degree sequence as you can.

6. (from LPC 2021) Consider your student ID number as a sequence of eight digits $d_1, d_2, \ldots, d_8$.
   For example if my student ID is 13712435 then I consider the sequence $1, 3, 7, 1, 2, 4, 3, 5$.

   Draw a picture of an undirected graph having degree sequence $d_1, d_2, d_3, \ldots, d_8$, or explain why no such graph exists.

Date: Week 10 workshop (Wednesday 4, Thursday 5, Friday 6 May).

[1] which should be 27

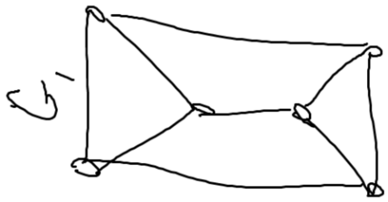
[2] You were allowed to use https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/powermod.html instead of repeated squaring to save some time for this LPC question.

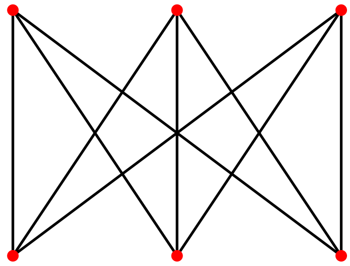
[3] What does *different* mean? We will learn a formal definition next week. For now, argue with your teammates about whether two graphs are essentially the same, or definitely not the same.

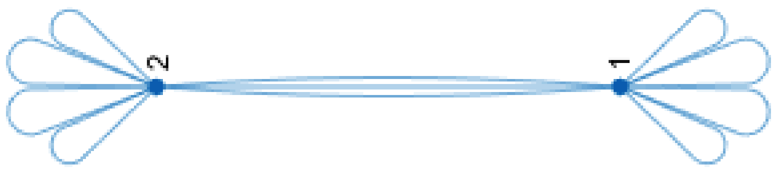
7. For each of the following graphs

   (a) compute the degree sequence

   (b) write an adjacency matrix







8. A graph is *planar* if a diagram of it can be draw on the plane (on the whiteboard) with no edges crossing. Decide whether the following graphs are planar or not (by trying to draw them without edges crossing): [4]

   (a) K_4
   (b) K_5
   (c) K_6
   (d) $K_{2,2}$
   (e) $K_{2,3}$
   (f) $K_{3,3}$

9. (a) Draw a picture of an undirected graph having degree sequence $1, 1, 2, 4, 4$, or explain why no such graph exists.

   (b) Is your graph in part (a)
      (i) Connected?
      (ii) Planar?
      (iii) Simple (no loops or multi-edges)?

10. (a) Draw a picture of an undirected graph having adjacency matrix
$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 2 & 1 \end{bmatrix}$$
, or explain why no such graph exists.

   (b) Is your graph in part (a)
      (i) Connected?
      (ii) Planar?
      (iii) Simple (no loops or multi-edges)? [5]

END OF WORKSHEET

[4] we will learn how to prove a graph is *not* planar in week 12. For now, you can prove when they *are* planar by drawing them, but proving they are *not* takes more effort.

[5] Notice anything fishy about these two questions?: we will learn formally what it means for two graphs to be *essentially the same* next week.

Brief solutions:

1. (a) $\varphi(55) = \varphi(5)\varphi(11) = 4.10 = 40$
   (b) so she needs the inverse of 17 mod 40 which is (Euclidean algorithm)

$$\begin{aligned} 40 &= 2.17 + 6, \\ 17 &= 2.6 + 5, \\ 6 &= 1.5 + 1 \end{aligned}$$

   so

$$\begin{aligned} 1 &= 6 - 5 \\ &= 6 - (17 - 2.6) \\ &= 3.6 - 17 \\ &= 3(40 - 2.17) - 17 \\ &= 3.40 - 7.17 \end{aligned}$$

   so the inverse is $-7 \equiv 33$.

   (c) Bob sends $27^{17} \equiv 47 \mod 55$.

   (d) Alice computes $c^d = 47^{33} \equiv 27$.

2. $143 = 13.11$ so $\varphi(143) = 12.10 = 120$. Inverse: Euclidean algorithm –

$$\begin{aligned} 120 &= 9.13 + 3 \\ 13 &= 4.3 + 1 \end{aligned}$$

Backwards:

$$\begin{aligned} 1 &= 13 - 4.3 \\ &= 13 - 4(120 - 9.13) \\ &= 13 + 36.13 - 4.120 \\ &\equiv 37.13 \end{aligned}$$

so inverse is $d = 37$. Check: $37.13 = 481 = 4.120 + 1$ correct.

Bob sends $c = 4 = ([m^e]_{143})$ so Alice decodes by computing $[c^d]_{143} = [4^{37}]_{143}$: Repeated squaring –

$$\begin{aligned} 4^2 &= 16 \\ 4^4 &= 16^2 = 256 \equiv 113 \equiv -30 \\ 4^8 &\equiv (-30)^2 = 900 = 858 + 42 \equiv 42 \\ 4^{16} &\equiv (42)^2 = 1764 = 1716 + 48 \equiv 48 \\ 4^{32} &\equiv (48)^2 = 2304 \equiv 16 \end{aligned}$$

so $4^{37} = 4^{32}4^4 4^1 \equiv 16.(-30).4 = (-480).4 \equiv 92.4 = 368 \equiv 82$.

Answer: $m = 82$.

Check: Bob would have done: $82^e = 82^{13}$ – repeated squaring to check.

$$82^2 = 6724 = 47.143 + 3 \equiv 3$$

$$82^4 = 9$$

$$82^8 = 81$$

so

$$82^{13} = 82^8.82^4.82^1 \equiv 81.9.82 = 729.82 \equiv 14.82 = 1148 = 1144 + 4 \equiv 4$$

correct!!

3. (a) 31.41 so $\varphi(1271) = 30.40 = 1200$. Eucl alg backwards gives $d = -229 \equiv 971$.

   (b) $[c^d]_n = [11^{971}]_{1271} = 427$ using powermod website.

4. (a) Let v be a vertex of a graph and E the edge set. Set a counter $\deg(v) == 0$. For each edge $e \in E$, if e is associated to $\{v\}$ then
$$\deg(v) \leftarrow \deg(v) + 2,$$
and if e is associated to $\{v, w\}$ with $w \neq v$ then
$$\deg(v) \leftarrow \deg(v) + 1.$$
This procedure outputs $\deg(v)$.

   (b) A sequence of edges associated to sets $\{x, v_1\}, \{v_1, v_2\}, \dots, \{v_n, y\}$ where each v_i is different from all other v_j and from x and y. (Note x, y are allowed to be the same vertex).

   (c) If G is a graph with $V = \{1, 2, \dots, n\}$ then $A = (a_{ij})_{1\leqslant i,j\leqslant n}$ where a_{ij} = number of edges associated to $\{i, j\}$.

7. (a)
   - 3, 3, 3, 3, 3, 3
   - 3, 3, 3, 3, 3, 3
   - 11, 11 (remember loops add 2 for the degree).

   (b) G_1: $\begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$ (depends on which order you label your graph)

   G_3: $\begin{bmatrix} 4 & 3 \\ 3 & 4 \end{bmatrix}$

8. (a), (d), (e) are planar, the others are not (we will prove in week 12).

3. (3 marks)
   (a) Alice constructs an RSA system by choosing $n = 1271$ and $e = 131$. Find d. Show all steps.

$1271 = 31 \cdot 41$ so $\phi(1271) = 30 \cdot 40 = 1200$

$1200 = 9 \cdot 131 + 21$
$131 = 6 \cdot 21 + 5$
$21 = 4 \cdot 5 + 1$

Backwards: $1 = 21 - 4(131 - 6 \cdot 21)$
$= 25 \cdot 21 - 4 \cdot 131$
$= 25(1200 - 9 \cdot 131) - 4 \cdot 131$
$= 25 \cdot 1200 - 229 \cdot 131$

↑ inverse mod $\phi(1271)$

$d = 1200 - 229$
$= 971$.

   (b) Bob sends a message encoded as $c = 11$ to Alice. What was his message m? Show all steps.[2]

(b) $c = [m^e]_n = [m^{131}]_{1271}$

$c^d = [m^{ed}]_n = [m^1]_n$

$[11^{971}]_{1271}$ using powermod $= 427$

$\therefore m = 427$

END OF LPC6

[2]Hint: you may use https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/powermod.html instead of repeated squaring to save some time. Show a screenshot of your calculation if you do.

MATH 139 **SPRING 2003**

PowerMod Calculator

Computes (base)$^{\text{(exponent)}}$ mod (modulus) in log(exponent) time.

Base:	Exponent:	Modulus:
11	971	1271
Compute	b^e MOD m =	427

The program is written in JavaScript, and runs on the client computer. Most implementations seem to handle numbers of up to 16 digits correctly.

Check: If I was Bob:

I want to send $m = 427$

$$c = [427^e]_{1271} = [427^{131}]_{1271}$$

(powermod) $= 11$ ✓

MATH 139 **SPRING 2003**

PowerMod Calculator

Computes (base)$^{\text{(exponent)}}$ mod (modulus) in log(exponent) time.

Base:	Exponent:	Modulus:
427	131	1271
Compute	b^e MOD m =	11

The program is written in JavaScript, and runs on the client computer. Most implementations seem to handle numbers of up to 16 digits correctly.