SI 120 Discrete Mathematics (Spring 2021), Final Exam

Name (in Chinese): _____

ID#: _____

Email: _____**@shanghaitech.edu.cn**

Instructions

- Time: 8:00–10:00am (120 minutes)
- This exam is closed-book, you may bring nothing but a pen. Put all the study materials and electronic devices into your bag and put your bag in the front, back, or sides of the classroom.
- You can write your answers in either English or Chinese.
- Two blank pieces of paper are attached, which you can use as scratch paper. Raise your hand if you need more paper.

1 Multiple choice (50 pt)

Each question has only one correct answer. *Write your answers in the table below.*

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20

1. Let $a, b \in \mathbb{Z}$ and $a \neq 0$. Which of the following statement is correct?

   A. a divides b if there is an integer $c \in \mathbb{Z}$ such that $a = bc$.

   B. $n \in \mathbb{Z}^+$ is not a prime, then n is called a composite.

   C. The set $\mathbb{Z}_{1999}^*$ has 1998 elements.

   D. According to FTA, every integer $n \geqslant 1$ cound be uniquely written as $n = p_1^{e_1} \cdots p_r^{e_r}$ where $p_1, ..., p_r$ are distinct primes and $e_1, ..., e_r \geq 1$.

2. Which of the following statement is correct?

   A. If a, b are integers, then there exists integers q, r such that $a = bq + r$ and $0 < r < b$, where $q = \lfloor \frac{a}{b} \rfloor$.

   B. $\lfloor \lfloor x \rfloor + 0.5 \rfloor = \lfloor x + 0.5 \rfloor$ for all real number x.

   C. If I_1 and I_2 are ideals of $\mathbb{Z}$, then $I_1 + I_2$ is also an ideal of $\mathbb{Z}$.

   D. Suppose p is a prime and $p|ab$, then $p|a$ and $p|b$.

3. Which of the following is not equivalence relation?

   A. $S = \{(x, y) : x, y \in \mathbb{R}, x \equiv y \mod 1997\}$ on $\mathbb{R}$.

B. $S = \{(x, y) : x, y \in \mathbb{R}, x - y \in \mathbb{Z}\}$ on $\mathbb{R}$.

C. $S = \{(x, y) : x, y \in \mathbb{R}, x + y \in \mathbb{Z}\}$ on $\mathbb{R}$.

D. $S = \{(x, y) : x, y \in \mathbb{R}, x - y \in \mathbb{Q}\}$ on $\mathbb{R}$.

4. Which of the following is equivalent to $\mathbb{Z}_8^*$?

   A. $\{[0]_8, [1]_8, [2]_8, [3]_8, [4]_8, [5]_8, [6]_8, [7]_8\}$

   B. $\{[0]_8, [1]_8, [3]_8, [5]_8, [7]_8\}$

   C. $\{[-1]_8, [3]_8, [5]_8, [-7]_8\}$

   D. $\{[-1]_8, [-3]_8, [-5]_8, [-6]_8, [-7]_8\}$

5. Let $\phi(n)$ be the Euler's Phi function, and $n = 5^3 \times 7 \times 13^2$. Then $\phi(n) =$

   A. 93400.

   B. 93500.

   C. 93600.

   D. 93700.

6. Let $a = 301$ and $n = 12345$. Which of the following is an inverse of $[a]_n$?

   A. $[3046]_n$.

   B. $[3056]_n$.

   C. $[3066]_n$.

   D. $[3076]_n$.

7. Which of the following statement is correct?

   A. Let p and q be any two primes and $n = pq$, then $\phi(n) = (p - 1)(q - 1)$.

   B. According to the Euler's Theorem, if $n \geq 1$ and $\alpha \in \mathbb{Z}_n$, then $\alpha^{\phi(n)} \equiv 1 (\text{mod } n)$.

   C. If $n = p_1^{e_1} \cdots p_k^{e_k}$ for distinct primes $p_1, ..., p_k$ and integers $e_1, ..., e_k \geq 1$, then $\phi(n) = n(1 - p_1) \cdots (1 - p_k)$.

   D. According to Fermat's Little Theorem, if p is a prime and $\alpha \in \mathbb{Z}_p$, then $\alpha^p \equiv \alpha (\text{mod } p)$.

8. Which of the following statements about RSA cryptosystem is correct?

   A. The two primes p and q are computed by deterministic algorithm.

   B. Given $N = pq$, we can factor it in $O(\sqrt{N})$ time, which is polynomial, so we can factor it efficiently.

   C. Choosing a small d in public key would speed up the encryption.

   D. We can compute $a^e (\text{mod } n)$ in $O\left(\ell(e)\ell(n)^2\right)$ time.

9. Which of the following statement about prime theory is correct?

   A. Let $\pi(x)$ be the number of primes $\leq x$. Then $\lim_{x \to \infty} \frac{\pi(x)}{2x/\ln x} = 1$.

   B. When the integer x is large enough, there are more prime numbers than composite numbers in the set $\{1, 2, ..., x\}$.

   C. The Miller-Rabin test will always output the correct result.

   D. Let $\mathbb{P}_n = \{p \in \mathbb{P} : \ell(p) = n\}$, then $|\mathbb{P}_n| \geq \frac{2^n}{n \ln 2} \left(\frac{1}{2} + O\left(\frac{1}{n}\right)\right)$ when $n \to \infty$.

10. Which of the following statement is incorrect?

    A. An public-key encryption system is said to be secure if it is difficult to learn m from pk, c if sk is unknown.

    B. The best known algorithm for the factoring problem has subexponential complexity.

    C. Diffie–Hellman key exchange is a method of securely exchanging cryptographic keys over a public channel.

D. Suppose $A = g^a \pmod{p}$. Given A and g, it is easy to compute $a = \log_g A$ if the numbers are large.

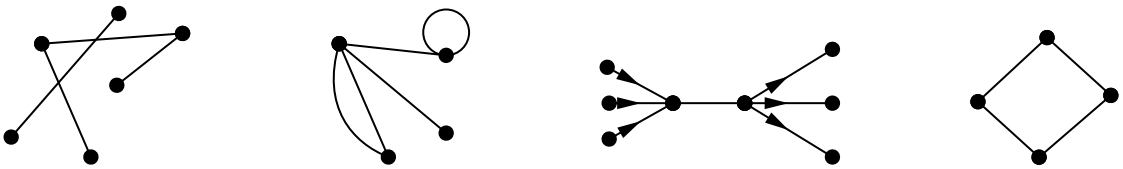
11. Which of the following statements is correct?

A. Graph (a) is a simple graph.

B. Graph (b) is a multigraph.

C. Graph (c) is a directed graph.

D. Graph (d) is a mixed graph.



(a) (b) (c) (d)

12. Which of the following statements is not correct?

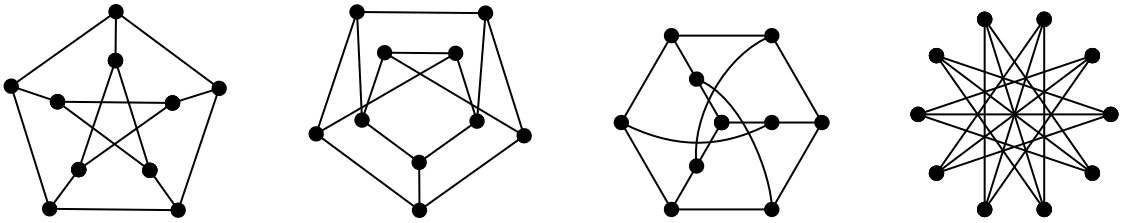
A. Graph Q_{2021} is bipartite.

B. Let G be a simple graph. If $\lambda(G) < 100$, then G is not 100-connected.

C. Let G be a simple graph with at least two vertices. Then G has at least two vertices that are not cut vertices.

D. Let G be a simple graph with 618 vertices and 18 connected components. Then G has at most 179700 edges.

13. Which one of the following graphs is not isomorphic to the others?



A. B. C. D.

14. Which of the following statements is not correct?

A. There are 4 non-isomorphic simple graphs with 5 vertices and 3 edges.

B. There are 11 non-isomorphic simple graphs with 4 vertices.

C. There are 2 non-isomorphic trees with 4 vertices.

D. There are 12 non-isomorphic trees with 7 vertices.

15. Which of the following statements is not correct?

A. Suppose that a connected bipartite planar simple graph has e edges and 99 vertices. Then $e \leq 194$.

B. There exists a connected planar simple graph with 52 edges and 32 vertices contains no simple circuits of length 4 or less.

C. There exists a complete matching from $U = \{u_1, u_2\}$ to $V = \{v_1, v_2, v_3\}$ in Figure 1.

D. A simple graph that has a circuit with an odd number of vertices in the circuit cannot be colored using two colors.

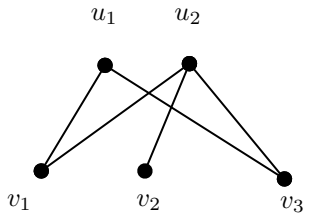


Figure 1: Matching

16. There is a counterfeit coin among 128 coins. This counterfeit coin is heavier than the other coins. The minimum number of weightings with a pan balance scale needed to find the counterfeit coin is?

    A. 5

    B. 6

    C. 7

    D. 8

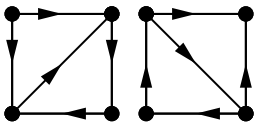
17. In the following graphs:

    A. Graph (a) is strongly connected, graph (b) is not strongly connected.

    B. Graph (a) is not strongly connected, but graph (b) is strongly connected.

    C. Both graph (a) and (b) are strongly connected.

    D. Neither graph (a) nor (b) is strongly connected.



18. If G is a planar graph with 3 connected components, 12 faces and 20 edges, then G has _____ vertices.

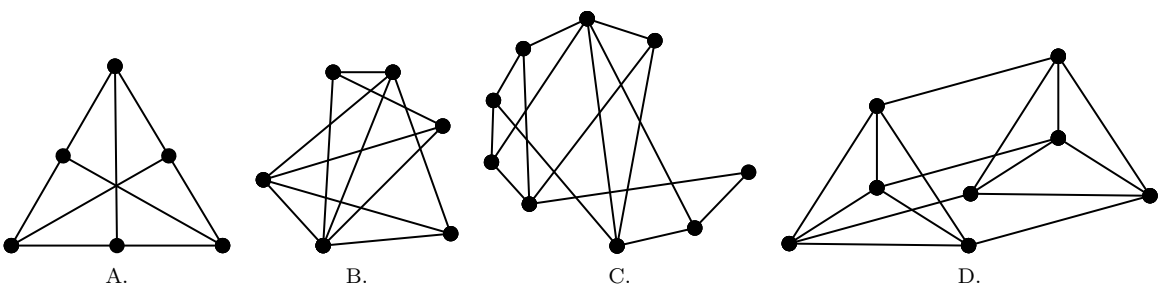
    A. 10

    B. 11

    C. 12

    D. 13

19. Which of the following graphs is planar?



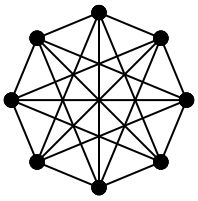
20. What is the chromatic number of the following graph?

A. 3

B. 4

C. 5

D. 6



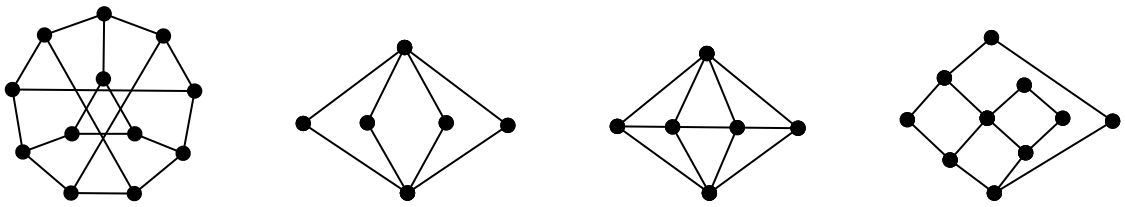
Solution:

1	2	3	4	5	6	7	8	9	10
C	C	C	C	C	D	D	D	D	D
11	12	13	14	15	16	17	18	19	20
A	D	D	D	B	A	D	C	B	B

2 Filling the Blank. (20pt)

1. Suppose that Alice and Bob are doing Diffie-Hellman key exchange. Alice sent a message $(p, g, A) = (13, 7, 5)$ to Bob; Bob sent a message $B = 10$ to Alice. At the end of the protocol, Alice will output a secret key k_A; Bob will output a secret key k_B. Then $k_A = k_B =$ _____.

2. Which of the following graph(s) have/has Hamilton circuit? _____.



A B C D

3. Given Figure 2. Let x be the number of paths from a to b with length 4, y be the number of paths from e to c with length 4. Then $xy =$ _____.

4. Suppose that m is a positive integer with $m \geq 2$. An m-ary Huffman code for a set of N symbols can be constructed analogously to the construction of a binary Huffman code. At the initial step, $((N-1) \bmod (m-1))+1$ trees consisting of a single vertex with least weights are combined into a rooted tree with these vertices as leaves. At each subsequent step, the m trees of least weight are combined into an m-ary tree. Tree with larger probability will be placed at left. Using the symbols 0, 1, and 2 use ternary ($m = 3$) Huffman coding to encode these letters with the given frequencies: $A : 0.25, E : 0.30, N : 0.10, R : 0.05, T : 0.12, Z : 0.18$.

   The code of the message $ENTER$ is _____.

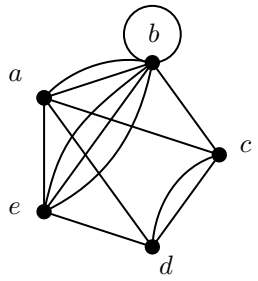


Figure 2: Number of paths

Solution:

1. 12
2. CD
3. 29200
4. 1010021011

3 Calculation (10 pt)

Suppose $N = 13 \times 17 = 221$ and $e = 53$. Let $pk = (N, e)$ be the public key of RSA. Decrypt the ciphertext $c = 56$ under pk.

Solution:

According to the definition, we have $\phi(n) = (p-1)(q-1) = 192$.

As $d \cdot e = 1 \pmod{\phi(n)}$, we could conclude that $\gcd(\phi(n), e) = 1$. By EEA, it is easy to calculate that $d = 29$.

By square and multiply, we could calculate that $m = c^d \mod N = 88$.

4 Graph Coloring (10 pt)

Show that every planar graph G can be colored using five or fewer colors. (You can not use the 4-coloring theorem.)

Solution:

We use induction on the number of vertices of the graph. Every graph with five or fewer vertices can be colored with five or fewer colors, because each vertex can get a different color. That takes care of the basis case(s). So we assume that all graphs with k vertices can be 5-colored and consider a graph G with $k+1$ vertices. By Corollary 2 in Section 10.7 in textbook, G has a vertex v with degree at most 5. Remove v to form the graph G'. Because G' has only k vertices, we 5-color it by the inductive hypothesis. If the neighbors of v do not use all five colors, then we can 5-color G by assigning to v a color not used by any of its neighbors. The difficulty arises if v has five neighbors, and each has a different color in the 5-coloring of G'. Suppose that the neighbors of v, when considered in clockwise order around v, are a, b, c, m, and p. (This order is determined by the clockwise order of the curves representing the edges incident to v.) Suppose that the colors of the neighbors are azure, blue, chartreuse, magenta, and purple, respectively. Consider the azure-chartreuse subgraph (i.e., the vertices in G colored azure or chartreuse and all the edges between them). If a and c are not in the same component of this graph, then in the component containing a we can interchange these two colors (make the azure vertices chartreuse and vice versa), and G' will still be properly colored. That makes a chartreuse, so we can now color v azure, and G has been properly colored. If a and c are in the same component, then there is a path of vertices alternately colored azure and chartreuse joining a and c. This path together with edges av and vc divides the plane into two regions, with b in one of them and m in the other. If we now interchange blue and magenta on all the vertices in the same region as b, we will still have a proper coloring of G', but now blue is available for v. In this case, too, we have found a proper coloring of G. This completes the inductive step, and the theorem is proved.

5 Tree (10 pt)

Either give m for a full m-ary tree with 84 leaves and height 3, where m is a positive integer, or show that no such tree exists.

Solution:

No such tree exists by Theorem 4 in textbook 11.1 because it is impossible for $m = 2$ or $m = 84$.