ITB8832 Mathematics for Computer Science
Final Exam, first date: 18 December 2024

Last update: 3 January 2025

Exercise 1 (8 points)

Four men and four women have the following lists of preferences:

Christof	Anezka, Abigail, Yennefer, Elaine
Geralt	Yennefer, Anezka, Elaine, Abigail
Guybrush	Abigail, Elaine, Yennefer, Anezka
John	Abigail, Anezka, Yennefer, Elaine

Abigail	Geralt, Christof, John, Guybrush
Anezka	Christof, Geralt, Guybrush, John
Elaine	Christof, Guybrush, John, Geralt
Yennefer	Guybrush, Geralt, Christof, John

Prove that there is a unique stable matching, and determine it. *Hint:* Look first for a couple that must appear in every stable matching.

Exercise 2 (10 points)

The set $N_{5,7}$ (read "enn five seven") of $5,7$-*averaged numbers* is defined recursively as follows:

- **Base case 1:** $0 \in N_{5,7}$
- **Base case 2:** $1 \in N_{5,7}$
- **Constructor case:** If $x, y \in N_{5,7}$, then $\dfrac{5x+7y}{12} \in N_{5,7}$.

Your tasks for this exercise:

1. (1 point) Explain why the definition of $N_{5,7}$ given above is ambiguous.

2. (3 points) Prove that $N_{5,7}$ contains an infinite strictly decreasing sequence.

3. (4 points) For every $n \in \mathbb{N}$ let H_n be the set of all and only those elements of $N_{5,7}$ by applying the constructor at most n times. For example, $H_0 = \{0, 1\}$ and: $H_1 = \left\{0, \frac{5}{12}, \frac{7}{12}, 1\right\}$. Prove that for every $n \geq 0$ there exists a surjective function from $(H_n)^2$ to H_{n+1}.

4. (2 points) Use points 2 and 3 to prove that $N_{2,3,7}$ is countably infinite.

   Important: You don't need to have solved points 2 and 3 to solve point 4, but you *must* use them.

Exercise 3 (10 points)

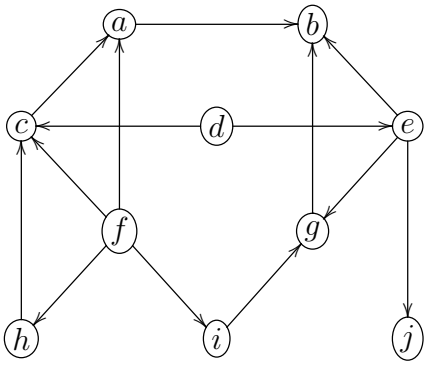
Let $p = 97$ and $q = 67$.

1. (3 points) Prove that $(e, n) = (455, 6499)$ is a valid RSA public key.

2. (7 points) Determine the private key d for the public key (e, n) of the previous point .

Exercise 4 (12 points)

The following directed acyclic graph D represents a list of tasks together with their priorities:



In addition to D, consider the simple graph G with the same set of vertices as D, and where $\langle u — v \rangle$ is an edge in G if and only if one between $\langle u \to v \rangle$ and $\langle v \to u \rangle$ is an edge in D.

1. (3 points) Construct a parallel schedule of minimum time for the set of tasks described by D, in the hypothesis that every task requires one unit of time.

2. (1 point) Does this set of tasks have a parallel schedule of minimum time with only two processors?

   This point is considered as solved if the schedule in your answer to point 1 uses only two processors.

3. (2 points) Prove that the chromatic number of G is 3.

4. (2 points) Prove that G is planar.

5. (4 points) Let now H be the graph obtained from G by first removing the vertex j and the incident edge $\langle e—j \rangle$, then adding the edges $\langle a—d \rangle$, $\langle b—d \rangle$, and $\langle h—i \rangle$. Construct two spanning trees of H with no edges in common.

Exercise 5 (20 points overall)

For each of the following questions, mark the only correct answer:

1. Which one of the following numbers is rational, but not integer?

   (a) $\log_9 27$.

   (b) $\log_3 27$.

   (c) $\log_9 26$.

2. Which one of the following subsets of $\mathbb{R}$ is *not* well ordered?

   (a) $A ::= \left\{ x \in \mathbb{R} \,\middle|\, x > \sqrt{17} \textbf{ and } \exists n \in \mathbb{N} \,.\, x = \dfrac{n}{n+1} \right\}$.

   (b) $B ::= \left\{ x \in \mathbb{Z} \,\middle|\, x > -\sqrt{17} \right\}$.

   (c) $C ::= \left\{ x \in \mathbb{Q} \,\middle|\, x > \sqrt{17} \right\}$.

3. Which one of the following propositional formulas is valid?

   (a) $((P \textbf{ implies } Q) \textbf{ implies } P) \textbf{ implies } P$.

   (b) $((P \textbf{ implies } Q) \textbf{ implies } Q) \textbf{ implies } P$.

   (c) $((P \textbf{ implies } Q) \textbf{ implies } Q) \textbf{ implies } Q$.

4. True or false: The predicate formula:

   $$\forall x \,.\, ((P(x) \textbf{ implies } Q(x)) \textbf{ or } (Q(x) \textbf{ implies } P(x)))$$

   has a counter-model.

5. Which one of the following is a preserved invariant for the Die Hard machine with jugs of 12 and 18 liters?

   (a) b is a multiple of 4.

   (b) Both ℓ and b are multiples of 4

   (c) Both ℓ and b are linear combinations of 12 and 18 with integer coefficients.

6. Consider the Mating Ritual for n men and n women with men as suitors. Which one of the following statements is true?

   (a) Every man is the optimal husband of his optimal wife.

   (b) If on a certain morning a woman is not on a man's list, then she will not be on the man's list on any of the following mornings.

   (c) The Mating Ritual finds the unique stable matching for the given set of preferences.

7. Which one of the following functions from $\{0,1\}^*$ to $\mathbb{N}$ is correctly defined by recursion?

   (a) $f(\langle a\,,\,s\rangle) = 1 + 2f(s)$ for every $a \in \{0,1\}$ and $s \in \{0,1\}^*$.

   (b) $g(\lambda) = 0$; $g(s) = 1 + 2g(\langle a\,,\,s\rangle)$; for every $a \in \{0,1\}$ and $s \in \{0,1\}^*$.

   (c) $h(\lambda) = 0$; $h(\langle a\,,\,s\rangle) = 1 + 2h(s)$ for every $a \in \{0,1\}$ and $s \in \{0,1\}^*$.

8. Which one of the following Nim games is a winning position for the first player?

   (a) $\mathrm{Nim}_{(26,55,45)}$.

   (b) $\mathrm{Nim}_{(36,55,35)}$.

   (c) $\mathrm{Nim}_{(46,55,25)}$.

9. True or false: There exists a set X such that $\mathrm{pow}(X)$ is countably infinite.

10. Which one of the following is true?

    (a) Every finite union of recognizable sets is recognizable.

    (b) Every countable union of recognizable sets is recognizable.

    (c) For every recognizable set L, the complement $\overline{L}$ is recognizable.

11. What is the remainder in the division of $100000^{183654} + 28^{73}$ by 19?

    (a) 0.

    (b) 1.

    (c) 10.

12. Let ϕ be Euler's function. Which one of the following is true for every positive integer n?

    (a) $a^{\phi(n)} \equiv 1 \pmod{n}$ for every positive integer a.

    (b) $a^n \equiv a \pmod{n}$ for every positive integer a.

    (c) $a^{\phi(n)} \equiv 1 \pmod{n}$ for every positive integer a such that $\gcd(a, n) = 1$.

13. Let (e, n) be an RSA public key. Which one of the following would allow us to efficiently reconstruct the private key d?

    (a) Knowing a prime factor of n.

    (b) Knowing a prime factor of $\phi(n)$.

    (c) Knowing the value $e^{-1} \pmod{n}$.

14. True or false: In every finite directed graph, the shortest closed walk through any given vertex is a cycle.

15. Which one of the following is true for every directed acyclic graph D on 88 vertices?

    (a) D has either a chain of size 14 or an antichain of size 7, and possibly both.

    (b) D has either a chain of size 14 or an antichain of size 8, and possibly both.

    (c) D has either a chain of size 16 or an antichain of size 7, and possibly both.

16. Which one of the following is true?

    (a) Every irreflexive relation is asymmetric.

    (b) Every asymmetric relation is irreflexive.

    (c) Every asymmetric relation is a strict partial order.

17. Let A be a nonempty set. How many binary relations on A are symmetric and asymmetric at the same time?

    (a) None.

    (b) One.

    (c) Two.

18. What is the chromatic number of a finite simple graph G?

    (a) The smallest positive integer k such that there exists a coloring of the vertices of G with k colors where no two adjacent vertices have the same color.

    (b) The smallest positive integer k such that there exists a coloring of the vertices of G with $k-1$ colors where no two vertices have the same color.

    (c) The largest positive integer k such that there exists a coloring of the vertices of G with k colors where no two adjacent vertices have the same color.

19. True or false: A simple graph with 47 vertices and 46 edges cannot contain a cycle.

20. Which one of the following simple graphs is *not* planar?

    (a) $K_{3,3}$.

    (b) $K_{4,2}$.

    (c) K_5 minus an edge.

This page intentionally left blank.

This page too.

Solution

Exercise 1

Let's follow the hint and observe that Christof and Anezka are each other's first choice, so they will be together in every stable matching. We can thus determine the other three couples based on the simpler lists of preferences:

Geralt	Yennefer, Elaine, Abigail
Guybrush	Abigail, Elaine, Yennefer
John	Abigail, Yennefer, Elaine
Abigail	Geralt, John, Guybrush
Elaine	Guybrush, John, Geralt
Yennefer	Guybrush, Geralt, John

There are at least two ways to determine the unique stable matching for this set of preferences. One is by showing that the Mating Ritual produces the same couples if run with men as suitors or with women as suitors. Another is by determining the only feasible wife for each man, *given the only feasible wives of the men considered previously.*

- With the Mating Ritual:

  A set of preferences has a unique stable matching if and only if the Mating Ritual produces the same couples when run with men as suitors and with women as suitors. With men as suitors:

  - On the first day:
    - In the morning, Guybrush and John become suitors of Abigail, and Geralt becomes a suitor of Yennefer.
    - In the afternoon, Abigail dismisses Guybrush.
    - In the evening, Guybrush removes Abigail from his list.
  - On the second day:
    - In the morning, Guybrush becomes a suitor of Elaine.
    - Every woman has exactly one suitor, and the couples are formed:

      (Geralt, Yennefer), (Guybrush, Elaine), (John, Abigail).

  With women as suitors:

  - On the first day:

    - In the morning, Elaine and Yennefer become suitors of Guybrush, and Abigail becomes a suitor of Geralt.
    - In the afternoon, Guybrush dismisses Yennefer.
    - In the evening, Yennefer removes Guybrush from her list.
  - On the second day:
    - In the morning, Yennefer becomes a suitor of Geralt.
    - In the afternoon, Geralt dismisses Abigail.
    - In the evening, Abigail removes Geralt from her list.
  - On the third day:
    - In the morning, Abigail becomes a suitor of John.
    - Every man has exactly one suitor, and the couples are formed: (Abigail, John), (Elaine, Guybrush), (Yennefer, Geralt).

  The couples are the same in both cases, so there is a unique stable matching.

- By determining the only feasible wife of every man, given the only feasible wives of the men considered previously:

  Yennefer is Geralt's first choice, so, if he has a different spouse, then he will try to form a rogue couple with her. This might not happen only if Yennefer was partnered with Guybrush, whom she prefers to Geralt. However, in this case, either Geralt is paired with Elaine and John with Abigail, or Geralt with Abigail and John with Elaine; in either case, Guybrush and Elaine form a rogue couple.

  We have thus proved that Yennefer is the only feasible wife for Geralt. Then we only need to consider the smaller set of preferences:

Guybrush	Abigail, Elaine	Abigail	John, Guybrush
John	Abigail, Elaine	Elaine	Guybrush, John

  But this smaller set of preferences has a unique stable matching: John with Abigail, Guybrush with Elaine.

We conclude that the only stable matching for the original set of preferences is:

(Christof, Anezka), (Geralt, Yennefer), (Guybrush, Elaine), (John, Abigail).

Exercise 2 (10 points)

1. The number 1 of $N_{5,7}$ can be obtained either as a base case, or by applying the constructor to $x = y = 1$.

2. We will prove by induction that $\left(\frac{5}{12}\right)^n \in N_{5,7}$ for every $n \in \mathbb{N}$.

   - **Base case:** $n = 0$. Then $\left(\frac{5}{12}\right)^0 = 1 \in N_{5,7}$
   - **Inductive step:** Assume that, for a certain $n \in \mathbb{N}$, it is $\left(\frac{5}{12}\right)^n \in N_{5,7}$ Then for the same n:

     $$\begin{aligned}\left(\frac{5}{12}\right)^{n+1} &= \frac{5}{12} \cdot \left(\frac{5}{12}\right)^n \\ &= \frac{5 \cdot \left(\frac{5}{12}\right)^n + 7 \cdot 0}{12}\end{aligned}$$

     is also an element of $N_{5,7}$.

3. Define $f_n : (H_n)^2 \to H_{n+1}$ as:

   $$f_n(x, y) = \frac{5x + 7y}{12}\,.$$

   Then f_n is a function, because on those pairs (x, y) where it is defined, its value is uniquely determined. Now let $a \in H_{n+1}$. By definition, a requires at most $n + 1$ applications of the constructor. If it requires *exactly* $n + 1$ applications, then it must have the form $a = \frac{5x + 7y}{12}$ for some $x, y \in N_{5,7}$ which require at most n applications of the constructor: in which case, $(x, y, z) \in (H_n)^2$. Otherwise, $a \in H_n$ and $a = f_n(a, a)$.

4. As $N_{5,7}$ has an infinite subset, it is infinite. As $N_{5,7} = \bigcup_{n \in \mathbb{N}} H_n$ is a countable union of finite sets, it is countable.

Exercise 3

1. The numbers p and q are distinct primes and their product is n. We have $\phi(97) = 96 = 2^5 \cdot 3$ and $\phi(67) = 66 = 2 \cdot 3 \cdot 11$, so $455 = 5 \cdot 7 \cdot 13$ has a multiplicative inverse modulo $\phi(n) = 96 \cdot 66 = 6336$.

2. To determine the private key, we use the Pulverizer:

a	b	$\text{rem}(a,b)$	$= a - \text{qcnt}(a,b) \cdot b$
6336	455	421	$= 6336 - 13 \cdot 455$
455	421	34	$= 455 - 421$
			$= 455 - (6336 - 13 \cdot 455)$
			$= -1 \cdot 6336 + 14 \cdot 455$
421	34	13	$= 421 - 12 \cdot 34$
			$= (6336 - 13 \cdot 455) - 12 \cdot (-1 \cdot 6336 + 14 \cdot 455)$
			$= 13 \cdot 6336 - 181 \cdot 455$
34	13	8	$= 34 - 2 \cdot 13$
			$= (-1 \cdot 6336 + 14 \cdot 455) - 2 \cdot (13 \cdot 6336 - 181 \cdot 455)$
			$= -27 \cdot 6336 + 376 \cdot 455$
13	8	5	$= 13 - 8$
			$= (13 \cdot 6336 - 181 \cdot 455) - (-27 \cdot 6336 + 376 \cdot 455)$
			$= 40 \cdot 6336 - 557 \cdot 455$
8	5	3	$= 8 - 5$
			$= (-27 \cdot 6336 + 376 \cdot 455) - (40 \cdot 6336 - 557 \cdot 455)$
			$= -67 \cdot 6336 + 933 \cdot 455$
5	3	2	$= 5 - 3$
			$= (40 \cdot 6336 - 557 \cdot 455) - (-67 \cdot 6336 + 933 \cdot 455)$
			$= 107 \cdot 6336 - 1490 \cdot 455$
3	2	1	$= (-67 \cdot 6336 + 933 \cdot 455) - (107 \cdot 6336 - 1490 \cdot 455)$
			$= -174 \cdot 6336 + 2423 \cdot 455$

Then the private key is $d = \text{rem}(2423, 6336) = 2423$.

Exercise 4

1. A schedule of minimum parallel time can be obtained by executing at time t all and only the tasks corresponding to vertices of depth t in D:

$$\begin{aligned} A_0 &= \{d, f\} \\ A_1 &= \{e, h, i\} \\ A_2 &= \{c, g, j\} \\ A_3 &= \{a\} \\ A_4 &= \{b\} \end{aligned}$$

2. The vertex j is maximal, so we can postpone it. The vertex e has depth 1 and is adjacent only to g, which has depth 2, to b, which is

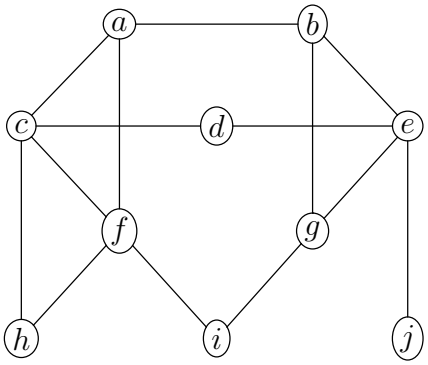


Figure 1: The simple graph G of Exercise 4.

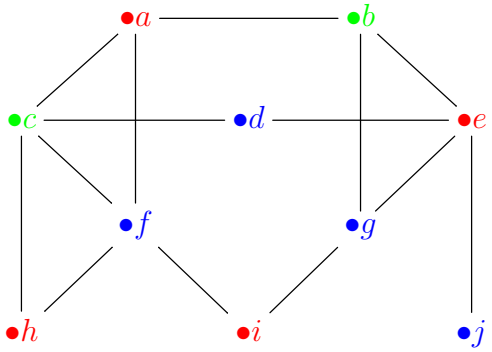


Figure 2: A 3-coloring of the simple graph G of Exercise 4.

maximal, and to j. Then we can postpone e and g as well and obtain the following two-processor schedule of minimum parallel time:

$$\begin{aligned} B_0 &= \{d, f\} \\ B_1 &= \{h, i\} \\ B_2 &= \{c, e\} \\ B_3 &= \{a, g\} \\ B_4 &= \{b, j\} \end{aligned}$$

3. The graph G has a cycle of length 3, so it is not 2-colorable. A 3-coloring of G is displayed in Figure 2.

4. A planar drawing of G is depicted in Figure 3.

5. Two spanning trees of H with no edges in common are depicted in Figure 4.

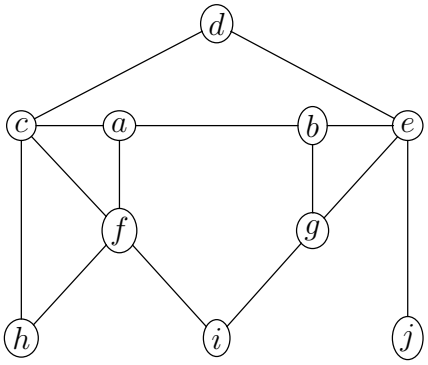


Figure 3: A planar drawing of the simple graph G of Exercise 4.

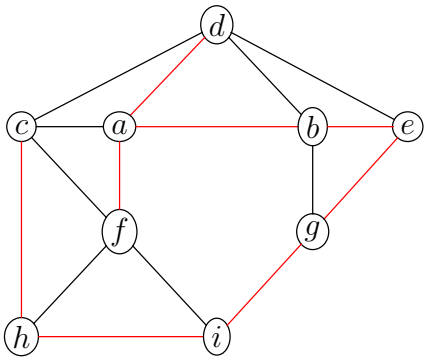


Figure 4: Two spanning trees with no edges in common for the simple graph H of Exercise 4. For greater clarity, the planar drawing of Figure 3 is used as a base.

Exercise 5

1. (a) **Yes:** $27 = 3^3$ and $9 = 3^2$, so $\log_9 27 = 3/2$.
   (b) **No:** $27 = 3^3$, so $\log_3 27 = 3$.
   (c) **No:** $\log_9 26 = \frac{1}{2}\log_3 26$ is the product of a rational number and an irrational one, so it is irrational.

2. (a) **No:** A is empty, and the empty set is well ordered, because it has no nonempty subsets, so it is vacuously true that every nonempty subset of the empty set has a smallest element.
   (b) **No:** B is a subset of $\mathbb{Z}$ bounded from below, so it is well ordered.
   (c) **Yes:** C contains the infinite decreasing sequence $6, 5+\frac{1}{2}, 5+\frac{1}{3}, 5+\frac{1}{4}, \ldots$

3. (a) **Yes:** this is called *Peirce's law*.
   (b) **No:** if P is false and Q is true, then the formula is false.
   (c) **No:** if P is true and Q is false, then the formula is false.

4. **False:** no matter what x is, if $P(x)$ is true, then $Q(x)$ **implies** $P(x)$ is true, and if $P(x)$ is false, then $P(x)$ **implies** $Q(x)$ is true, so the disjunction of the two is true in any case.

5. (a) **No:** from $(\ell, b) = (8, 3)$
   (b) **No:**
   (c) **Yes:** this is the same as saying that both ℓ and b are multiples of $\gcd(12, 18) = 6$.

6. (a) **No:** every man is the *pessimal* husband of his optimal wife (and the optimal husband of his pessimal wife).
   (b) **Yes:** if the woman is not on the man's list on one morning, it means that she has already rejected him on one of the previous days.
   (c) **No:** there are sets of preferences with more than two stable matchings.

7. (a) **No:** the base case $f(0)$ is missing.
   (b) **No:** recursion goes in the wrong direction.

(c) **Yes.**

8. (a) **No:** 26 XOR 55 XOR 45 = 0, so this is a winning position for the *second* player.

   (b) **Yes:** 36 XOR 55 XOR 35 = 48, so this is a winning position for the first player. Alternatively: 36, 55 and 35 are oddly many integers whose binary writings have 6 bits, so their Nim sum, whatever it is, must also have a binary writing with six bits.

   (c) **No:** 46 XOR 55 XOR 55 = 0, so this is a winning position for the *second* player.

9. **False:** the power set of any set is either finite, or uncountable.

10. (a) **Yes:** if for every $i \in [1..n]$ the program P_i recognizes the set L_i, then the program P which, when it receives in input an arbitrary string t, simulates in parallel the execution of all the P_i on t and halts if and only if one of the P_i halts, recognizes $\bigcup_{i=1}^{n} L_i$.

    (b) **No:** every finite subset of ASCII* is recognizable, but $\bigcup_{s \in \text{No-halt}} \{s\} =$ No-halt is not recognizable. The union is countable, because No-halt is a subset of ASCII*, which is countable. See also Exercise session 8.

    (c) **No:** $\overline{\text{No-halt}} = \{s \in \text{ASCII}^* \mid P_s \text{ halts on } s\}$ is recognizable, but its complement No-halt is not.

11. (a) **No:** see below.

    (b) **No:** see below.

    (c) **Yes:** 19 is prime, $\gcd(100000, 19) = \gcd(28, 19) = 1$, 183654 is a multiple of $\phi(19) = 18$, and $73 \equiv 1 \pmod{18}$, so
    $\text{rem}(100000^{183654} + 28^{73}, 19) = \text{rem}(1 + 28, 19) = 10$.

12. (a) **No:** for example, $\phi(9) = 6$, but $3^6 \equiv 0 \pmod 9$.

    (b) **No:** in the counterexample above, $3 \not\equiv 0 \pmod 9$, so $3^9 \not\equiv 3 \pmod 9$.

    (c) **Yes:** this is Euler's theorem.

13. (a) **Yes:** if p is a prime factor of n, then the other is $q = n/p$, and we can calculate first $\phi(n)$, then d.

    (b) **No:** in general, this piece of information is not useful. For example, 2 is *always* a prime factor of $\phi(n)$.

(c) **No:** in general, e and n don't need to be coprime, so that multiplicative inverse might not even exist.

14. **False:** the shortest closed walk *of positive length* is a cycle. The shortest closed walk is the empty walk.

15. (a) **Yes:** by Dilworth's lemma with $n = 88$ and $\ell = 13$.

    (b) **No:** for example, the DAG could be made of 6 chains of size 13 and one chain of size 10.

    (c) **No:** for example, the DAG could be made by 5 chains of size 15 and one chain of size 13.

16. (a) **No:** if $A = \{1, 2\}$ and xRy if and only if $x \neq y$, then R is irreflexive, but not asymmetric.

    (b) **Yes:** by contraposition, if for a certain $a \in A$ it is aRa, then for that same a and for $b = a$ it is aRb **and** bRa.

    (c) **No:** for example, the "beats" relation in the Rock-Paper-Scissors game is asymmetric, but not a strict partial order.

17. (a) **No:** see below.

    (b) **Yes:** the empty relation.

    (c) **No:** see above.

18. (a) **Yes.**

    (b) **No:** this is simply the number of vertices.

    (c) **No:** as soon as $k > |V(G)|$, such a coloring exists, so there is no largest such k.

19. **False:** the graph is not required to be connected, so it could be, for example, C_{46} plus an isolated vertex.

20. (a) **Yes:** $K_{3,13}$ clearly has a subgraph isomorphic to $K_{3,3}$, which is not planar.

    (b) **No:** $K_{2,n}$ is planar whatever $n \geq 1$ is.

    (c) **No:** see Lecture 15.