Mini-Quiz Apr. 6

Your name:_____

Circle the name of your TA/LA:

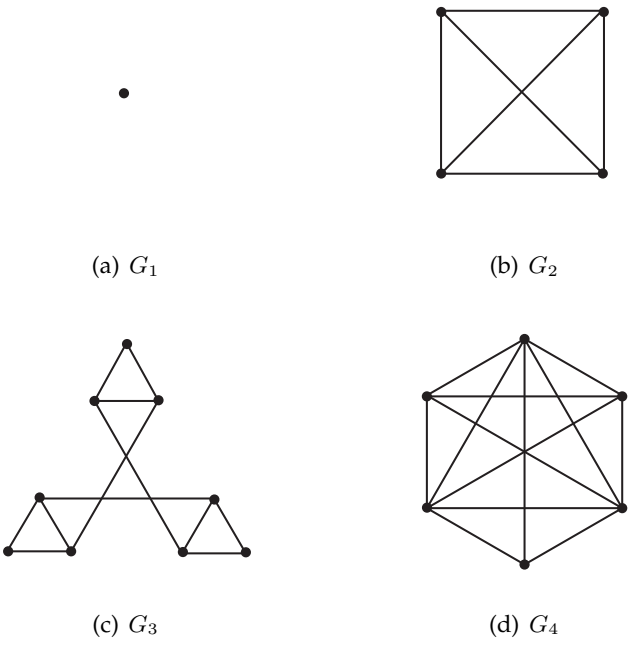
Chiyoun Jay Jeffrey Jessica Tina

- This quiz is **closed book**. Total time is 25 minutes.
- There are four (4) problems totalling 15 points.
- Write your solutions in the space provided. If you need more space, write on the back of the sheet containing the problem. Please keep your entire answer to a problem on that problem's page.
- GOOD LUCK!

DO NOT WRITE BELOW THIS LINE

Problem	Points	Grade	Grader
1	4		
2	5		
3	4		
4	2		
Total	15		

Problem 1 (4 points)**. (a)** Circle the graphs below that are planar (that *can be drawn* in the plane so that no edges cross).



(a) G_1 (b) G_2

(c) G_3 (d) G_4

(b) For each of the nonplanar graphs above, briefly explain why it is not planar.

Problem 2 (5 points)**.**

(a) (2.5 points) Circle all the valid statements about the greatest common divisor:

- Every common divisor of a and b divides $\gcd(a, b)$.
- $\gcd(ka, kb) = k \cdot \gcd(a, b)$ for all $k > 0$.
- If $\gcd(a, b) = 1$ and $\gcd(b, c) = 1$, then $\gcd(a, c) = 1$.
- If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.
- $\gcd(a, b) = \gcd(b, \mathrm{rem}(a, b))$.

(b) (2.5 points) Circle all the valid statements about equivalence mod n for $n \geq 1$:

- If $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.
- If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.
- If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.
- If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$.
- $\mathrm{rem}(a, n) \equiv a \pmod{n}$.

Problem 3 (4 points)**.**

(a) (1 point) Let $x = 13^2 17^5 23^{88} 31^{1000}$ and $y = 11^{53} 13^{12} 29^{35} 37^{28}$. What is the $\gcd(x, y)$?

(b) (1 point) For a given prime p, find *all* k in the range $\{0, 1, \ldots, p-1\}$ such that $k^2 \equiv 1 \pmod{p}$.

(c) (1 point) Find a value of k that makes the following statement true.

13^k is a multiplicative inverse of $13 \pmod{17}$.

(d) (1 point) What is the multiplicative inverse of 13 modulo 17? (We want the number between 0 and 16. If you get stuck working out the math, we will award partial credit if you explain how you would calculate this.)

Problem 4 (2 points)**.** Show how to use Euler's Formula and Lemmas 4.2 and 4.3 in the Appendix to prove that if a connected planar graph has $v \geq 3$ vertices and e edges, then

$$e \leq 3v - 6.$$

1 Appendix

Theorem 4.1 (Euler's Formula)**.** *If a connected graph has a planar embedding, then*

$$v - e + f = 2$$

where v is the number of vertices, e is the number of edges, and f is the number of faces.

Lemma 4.2. *In a planar embedding of a graph, each edge is traversed a total of two times by the faces of the embedding.*

Lemma 4.3. *In a planar embedding of a graph with at least three vertices, each face is of length at least three.*

Lemma 4.4. *Any subgraph of a planar graph is planar.*

Definition 4.5. a ***divides*** b iff $ak = b$ for some k. This is denoted $a \mid b$.

Theorem 4.6 (Division Theorem)**.** *Let n and d be integers such that $d > 0$. Then there exists a unique pair of integers q and r such that $n = qd + r$ and $0 \leq r < d$.*

The remainder r in the Division Theorem is denoted $\mathrm{rem}(n, d)$.

Definition 4.7. a ***is congruent to*** b ***modulo*** n iff $n \mid (a - b)$. This is denoted $a \equiv b \pmod{n}$.

Definition 4.8. A ***multiplicative inverse*** $\pmod{p}$ of a number x is another number x^{-1} such that:

$$x \cdot x^{-1} \equiv 1 \pmod{p}$$

Theorem (Fermat's (Little) Theorem)**.** *If p is prime and k is not a multiple of p, then*

$$k^{p-1} \equiv 1 \pmod{p}$$

Definition. The value of Euler's totient function, $\phi(n)$, is defined to be the number of positive integers less than n that are relatively prime to n.

Lemma (Euler Function Equations)**.** *If p is prime, then*

$$\phi(p^k) = p^k - p^{k-1} \qquad \text{for prime, } p, \text{ and } k > 0$$
$$\phi(mn) = \phi(m) \cdot \phi(n) \qquad \text{for } \gcd(m, n) = 1.$$

Theorem (Euler's Theorem)**.** *If k and n are relatively prime, then*

$$k^{\phi(n)} \equiv 1 \pmod{n}$$

The Pulverizer

Euclid's algorithm for finding the GCD of two numbers relies on repeated application of the equation:

$$\gcd(a, b) = \gcd(b, \mathrm{rem}(a, b))$$

For example, we can compute the GCD of 259 and 70 as follows:

$$\begin{array}{rcll} \gcd(259, 70) & = & \gcd(70, 49) & \text{since } \mathrm{rem}(259, 70) = 49 \\ & = & \gcd(49, 21) & \text{since } \mathrm{rem}(70, 49) = 21 \\ & = & \gcd(21, 7) & \text{since } \mathrm{rem}(49, 21) = 7 \\ & = & \gcd(7, 0) & \text{since } \mathrm{rem}(21, 7) = 0 \\ & = & 7. & \end{array}$$

The Pulverizer goes through the same steps, but requires some extra bookkeeping along the way: as we compute $\gcd(a, b)$, we keep track of how to write each of the remainders (49, 21, and 7, in the example) as a linear combination of a and b (this is worthwhile, because our objective is to write the last nonzero remainder, which is the GCD, as such a linear combination). For our example, here is this extra bookkeeping:

x	y	$\mathrm{rem}(x, y)$		$x - q \cdot y$
259	70	49	=	$259 - 3 \cdot 70$
70	49	21	=	$70 - 1 \cdot 49$
			=	$70 - 1 \cdot (259 - 3 \cdot 70)$
			=	$-1 \cdot 259 + 4 \cdot 70$
49	21	7	=	$49 - 2 \cdot 21$
			=	$(259 - 3 \cdot 70) - 2 \cdot (-1 \cdot 259 + 4 \cdot 70)$
			=	$\boxed{3 \cdot 259 - 11 \cdot 70}$
21	7	0		

We began by initializing two variables, $x = a$ and $y = b$. In the first two columns above, we carried out Euclid's algorithm. At each step, we computed $\mathrm{rem}(x, y)$, which can be written in the form $x - q \cdot y$. (Remember that the Division Algorithm says $x = q \cdot y + r$, where r is the remainder. We get $r = x - q \cdot y$ by rearranging terms.) Then we replaced x and y in this equation with equivalent linear combinations of a and b, which we already had computed. After simplifying, we were left with a linear combination of a and b that was equal to the remainder as desired. The final solution is boxed.