Name: Key

Directions: This test has 6 pages, each worth 10 points. The test is scored out of 50 points. Your lowest scoring page is dropped. Unless explicitly stated, answers to counting problems do not need to be simplified.

1. [~~2~~ 3 **points**] Find the <u>numerical value</u> of the coefficient of x^6y^9 in $(x+y)^{15}$.

$$C(15,6)=\binom{15}{6}=\frac{\overset{3}{\cancel{15}}\cdot\overset{7}{\cancel{14}}\cdot 13\cdot\overset{2}{\cancel{12}}\cdot 11\cdot\overset{5}{\cancel{10}}}{\cancel{6}\cdot\cancel{5}\cdot\cancel{4}\cdot\cancel{3}\cdot\cancel{2}}=7\cdot13\cdot11\cdot5=\boxed{5005}$$

2. [~~2~~ 3 **points**] Find the ~~numerical value~~ of the coefficient of $x^2y^6z^3$ in $(x+y+z)^{11}$.

$$\boxed{\frac{11!}{2!\,6!\,3!}}=\frac{11\cdot10\cdot9\cdot8\cdot7}{2!\cdot3!}=\frac{11\cdot10\cdot\overset{3}{9}\cdot\overset{2}{\cancel{8}}\cdot7}{\cancel{2}\cdot\cancel{3}\cdot\cancel{2}}=11\cdot10\cdot3\cdot2\cdot7=\boxed{4{,}620}$$

3. [~~3~~ 4 **points**] Find the coefficient of x^8 in $(5x-1)^{15}$. You do not need to simplify your answer.

$$\binom{15}{8}(5x)^8(-1)^7=\boxed{-\binom{15}{8}\cdot5^8}\cdot x^8$$

$$\text{or } \boxed{-C(15,8)\cdot5^8}$$

4. [**3 points**] Find the coefficient of $x^7y^3z^2$ in $(4x-2y+3z+1)^{20}$. You do not need to simplify your answer.

$$\frac{20!}{7!\cdot3!\cdot2!\cdot8!}(4x)^7(-2y)^3(3z)^2(1)^8$$

$$=\boxed{-\frac{20!}{7!\cdot3!\cdot2!\cdot8!}\cdot4^7\cdot2^3\cdot3^2}\,x^7y^3z^2$$

5. [**5 points**] Write gcd(48995, 2855) as a linear combination of 48995 and 2855. Show your work.

$$48995 = 17 \cdot 2855 + 460$$
$$2855 = 6 \cdot 460 + 95$$
$$460 = 4 \cdot 95 + 80$$
$$95 = 1 \cdot 80 + 15$$
$$80 = 5 \cdot 15 + 5$$
$$15 = 3 \cdot 5 + 0$$
$$\gcd(5,0) = 5.$$

$$\begin{aligned}
5 &= 80 - 5 \cdot 15 \\
&= 80 - 5(95 - 1 \cdot 80) \\
&= 6 \cdot 80 - 5 \cdot 95 \\
&= 6(460 - 4 \cdot 95) - 5 \cdot 95 \\
&= 6 \cdot 460 - 29 \cdot 95 \\
&= 6 \cdot 460 - 29(2855 - 6 \cdot 460) \\
&= 180 \cdot 460 - 29 \cdot 2855 \\
&= 180(48995 - 17 \cdot 2855) - 29 \cdot 2855 \\
5 &= \boxed{180 \cdot 48995 - 3089 \cdot 2855}
\end{aligned}$$

6. [**2 parts, 1 point each**] Let S be the set of all linear combinations of 21 and 15.

(a) On the number line below, circle the numbers that are in S.

$-7 \quad -6 \quad -5 \quad -4 \quad -3 \quad -2 \quad -1 \quad 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7$

(b) Find a very simple description of the set S.

S is the set of integers that are divisible by 3.

7. [**3 points**] The prime factorization of 14850 is given by $14850 = 2 \cdot 3^{\cancel{3}} \cdot 5^2 \cdot 11$. Find $\varphi(14850)$.

$$\varphi(14850) = \cancel{2} \cdot 3^{\cancel{3}\,2} \cdot 5^{\cancel{2}} \cdot \cancel{11} \cdot \left(\frac{1}{\cancel{2}}\right) \cdot \left(\frac{2}{\cancel{3}}\right) \cdot \left(\frac{4}{\cancel{5}}\right) \cdot \left(\frac{10}{\cancel{11}}\right)$$

$$= 3^2 \cdot 5 \cdot 2 \cdot 4 \cdot 10 = \boxed{3600}$$

8. **[2 parts, 5 points each]** In the RSA algorithm, let $p = 37$ and $q = 67$. Then $n = 2479$ and $\varphi(n) = 2376$. For the encryption key, pick $e = 17$.

(a) Use the Euclidean algorithm to find the decryption key d.

$$2376 = 139 \cdot 17 + 13$$
$$17 = 1 \cdot 13 + 4$$
$$13 = 3 \cdot 4 + 1$$
$$4 = 4 \cdot 1 + 0$$
$$\gcd = 1.$$

$$1 = 13 - 3 \cdot 4$$
$$= 13 - 3(17 - 1 \cdot 13)$$
$$= 4 \cdot 13 - 3 \cdot 17$$
$$= 4(2376 - 139 \cdot 17) - 3 \cdot 17$$
$$1 = 4 \cdot 2376 - 559 \cdot 17$$

$$\text{So } d = -559 \bmod 2376 = \boxed{1817}$$

(b) Encode $T = \cancel{42}\ \cancel{1207}\ 3$ using the public key (n, e).

Modulo 2479:
$$T^1 \equiv 1207$$
$$T^2 \equiv 1676$$
$$T^4 \equiv 1676 \cdot 1676 \equiv 269$$
$$T^8 \equiv 269 \cdot 269 \equiv 470$$
$$T^{16} \equiv 470 \cdot 470 \equiv 269$$
$$T^{17} \equiv 269 \cdot 1207 \equiv \boxed{2413}$$

$$(T)^1 \equiv 3$$
$$T^2 \equiv 3 \cdot 3 \equiv 9$$
$$T^4 \equiv 9 \cdot 9 \equiv 81$$
$$T^8 \equiv 81 \cdot 81 \equiv 6561 \equiv 1603$$
$$T^{16} \equiv 1603 \cdot 1603 \equiv 1365$$
$$T^{17} \equiv 1365 \cdot 3 \equiv \boxed{1616}$$

9. **[2 parts, 2 points each]** Let $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Express the following permutations as the composition of zero or more disjoint cycles; each cycle should have at least 2 elements.

(a) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 4 & 1 & 8 & 5 & 2 & 6 \end{pmatrix}$

$$\boxed{(1\ 3\ 4) \circ (2\ 7) \circ (5\ 8\ 6)}$$

(b) $(6\ 8) \circ (2\ 7\ 6\ 4) \circ (4\ 1\ 2\ 8\ 7)$

$$\boxed{(1\ 7\ 2\ 6\ 4)}$$

10. **[3 parts, 2 points each]** Let X be a set of size 10 and let $Y = \{1, 2, 3\}$.

(a) How many functions $f\colon X \to Y$ are there?

$$\boxed{3^{10}}$$

(b) How many one-to-one/injective functions $f\colon X \to Y$ are there?

$$\boxed{0}$$

(c) How many onto/surjective functions $f\colon X \to Y$ are there? *[Hint: For $j \in \{1, 2, 3\}$, let A_j be the set of all functions that map no elements in X to j. Count $|A_1 \cup A_2 \cup A_3|$ and use this to answer the question.]*

$$|A_1| = |A_2| = |A_3| = 2^{10}$$

$$|A_1 \cap A_2| = |A_2 \cap A_3| = |A_1 \cap A_3| = 1^{10}$$

$$|A_1 \cap A_2 \cap A_3| = 0$$

Inclusion/Excl: $|A_1 \cup A_2 \cup A_3| = 3 \cdot 2^{10} - 3 \cdot 1^{10} + 0 = 3 \cdot 2^{10} - 3$

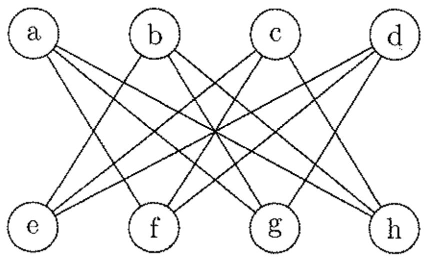
Surjective: $3^{10} - (3 \cdot 2^{10} - 3) = \boxed{3^{10} - 3 \cdot 2^{10} + 3 = 55980}$

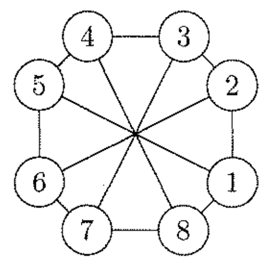
11. ~~[**2 points**] Let $f\colon \mathbb{R} \to \mathbb{R}$ be given by $f(x) = 4x + 9$. Is f a bijection? If f is a bijection, find the inverse of f. If not, prove that f is not a bijection.~~

$y = 4x+9$ | $\frac{y-9}{4} = x$ | Yes, f is a bijection and $\boxed{f^{-1}(y) = \frac{y-9}{4}}$

$y - 9 = 4x$

12. [~~4~~ 5 **points**] Decide if the following graphs are isomorphic. If they are isomorphic, give the function that establishes the isomorphism. If not, explain why.

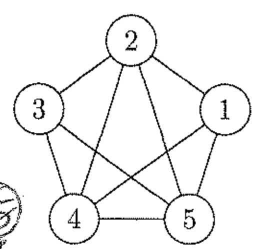




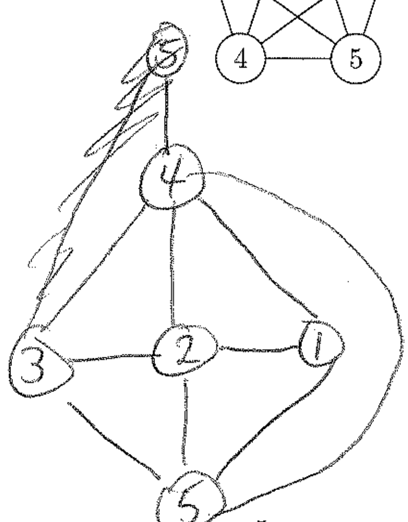
They are not isomorphic since left graph is bipartite and the right graph has 5-cycles.

Prove that the following graph is planar.

13. [~~4~~ 5 **points**] Deter~~mine if the graph is planar~~ (by finding ~~a planar~~ drawing) or nonplanar (by finding a subgraph that is a subdivision of $K_{3,3}$ ~~or K_5~~).



Planar:



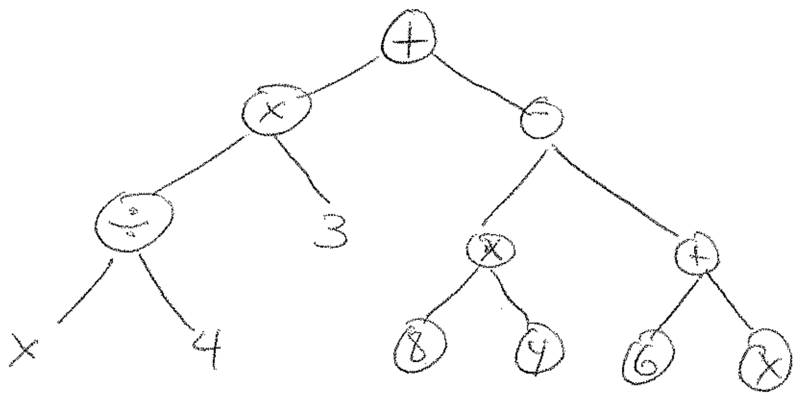
14. (a) [**2 points**] What is the maximum number of edges possible in a simple planar graph with 100 vertices?

$3 \cdot 100 - 6 = \boxed{294}$

(b) [**4 points**] Use part (a) to prove that every simple planar graph on 100 vertices has a vertex of degree at most 5.

Suppose for a contradiction that G does not have a vertex of degree 6. Then the degree sum is $6 \cdot 100 = 600$, so G has $\frac{600}{2} = 300$ edges. But since $300 > 294$, G can not be planar. ☐

15. [**2 points**] Draw the expression tree for $[(x \div 4) \cdot 3] + [(8 \cdot y) - (6 + x)]$.



16. [**2 points**] Draw the decision tree for sequential search on a list of three elements.