

NAME (1 pt): _____

TA & section #(1 pt): _____

Name of Neighbor to your left (1 pt): _____

Name of Neighbor to your right (1 pt): _____

Instructions: This is a closed book, closed notes, closed calculator, closed computer, closed network, open brain exam.

You get one point each for filling in the 4 lines at the top of this page. All other questions are worth 10 points. Since all questions have equal weight, do the questions you find easiest first.

If you start taking this exam, you have to turn it in.

Write all your answers on this exam. If you need scratch paper, ask for it, write your name on each sheet, and attach it when you turn it in (we have a stapler).

1	
2	
3	
4	
5	
Total	

Question 1) (10 points) From a group of 2 freshman (Sam and Pam), 3 sophomores (Will, Bill, and Jill) and 4 professors (Jones, Stones, Clones, and Bones) we wish to arrange a picture of 5 of them standing in a row. How many ways are there to arrange the 5 people in a photograph under the following conditions (each set of conditions is independent of the others). You may leave expressions like $C(20,10)$, or $13!$ unsimplified in your answers.

1. No conditions: any 5 people may appear in any order

Answer: $P(2+3+4,5) = P(9,5) = 9!/4! = 15120$

2. There must be exactly 3 faculty in the photograph.

Answer: ($\#$ ways to pick 3 locations for a professor) * ($\#$ ways to arrange 3 professors in order) * ($\#$ ways to fill remaining 2 slots) = $C(5,3)*P(4,3)*P(2+3,2) = 4800$

3. A freshman must appear directly to the right of a sophomore, and that sophomore directly to the right of a professor in the picture.

Answer: ($\#$ places to start sequence freshman/sophomore/professor) * ($\#$ ways to pick the freshman) * ($\#$ ways to pick the sophomore) * ($\#$ ways to pick the professor) * ($\#$ ways to fill in remaining 2 slots) = $3 * 2 * 3 * 4 * P(2+3+4-3,2) = 2160$

Question 1) (10 points) From a group of 3 boys (Joe, Bill and Lou), 3 girls (Zoe, Jill and Sue) and 4 school teachers (Dingle, Pringle, Zingle, and Single) we wish to arrange a picture of 5 of them standing in a row. How many ways are there to arrange the 5 people in a photograph under the following conditions (each set of conditions is independent of the others). You may leave expressions like $C(20,10)$, or $13!$ unsimplified in your answers.

1. No conditions: any 5 people may appear in any order.

Answer: $P(3+3+4,5) = P(10,5) = 10!/5! = 30240$

2. There must be exactly 2 school teachers in the photograph.

Answer: ($\#$ ways to pick 2 locations for a teacher) * ($\#$ ways to arrange 2 teachers in order) * ($\#$ ways to fill remaining 3 slots) = $C(5,2)*P(4,2)*P(3+3,3) = 14400$

3. A boy must appear directly to the right of a girl, and that girl directly to the right of a teacher in the picture.

Answer: ($\#$ places to start sequence boy/girl/teacher) * ($\#$ ways to pick the boy) * ($\#$ ways to pick the girl) * ($\#$ ways to pick the teacher) * ($\#$ ways to fill in remaining 2 slots) = $3 * 3 * 3 * 4 * P(3+3+4-3,2) = 4536$

Question 1) (10 points) From a group of 4 goats (Billy, Willy, Jilly and Silly), 3 geese (Honker, Zonker and Wonker), and 4 shepherds (Hansel, Gretel, Siegfried, and Brunhilda) we wish to arrange a picture of 5 of them standing in a row. How many ways are there to arrange the 5 creatures in a photograph under the following conditions (each set of conditions is independent of the others). You may leave expressions like $C(20,10)$ or $13!$ unsimplified in your answers.

1. No conditions: any 5 creatures may appear in any order.

Answer: $P(4+3+4,5) = P(11,5) = 11!/6! = 55440$

2. There must be exactly 3 goats in the photograph.

Answer: ($\#$ ways to pick 3 locations for a goat) * ($\#$ ways to arrange 3 goats in order) * ($\#$ ways to fill remaining 2 slots) = $C(5,3)*P(4,3)*P(3+4,2) = 10080$

3. A goose must appear directly to the right of a shepherd, and that shepherd directly to the right of a goat in the picture.

Answer: ($\#$ places to start sequence goose/shepherd/goat) * ($\#$ ways to pick the goose) * ($\#$ ways to pick the shepherd) * ($\#$ ways to pick the goat) * ($\#$ ways to fill in remaining 2 slots) = $3 * 3 * 4 * 4 * P(4+3+4-3,2) = 8064$

Question 2) (10 points) What $n < 0$ that is smallest in absolute value satisfies $2n \bmod 5 = 3$ and $3n \bmod 4 = 2$?

Answer: Since $2 \cdot 3 \equiv 1 \pmod{5}$, we can rewrite $2n \bmod 5 = 3$ as

$$3 \cdot 2n \bmod 5 = n \bmod 5 = 3 \cdot 3 \bmod 5 = 4.$$

Since $3 \cdot 3 \equiv 1 \pmod{4}$, we can rewrite $3n \bmod 4 = 2$ as

$$3 \cdot 3n \bmod 4 = n \bmod 4 = 3 \cdot 2 \bmod 4 = 2.$$

To solve $n \bmod 5 = 4$ and $n \bmod 4 = 2$ we use the Chinese Remainder Theorem to get $n = (4 \cdot 4 \cdot 4 + 2 \cdot 1 \cdot 5) \bmod 4 \cdot 5 = 14$.

Subtracting $5 \cdot 4 = 20$ to get the negative solution with smallest absolute value yields $n = -6$.

Question 2) (10 points) What $m < 0$ that is smallest in absolute value satisfies $4m \bmod 7 = 1$ and $3m \bmod 5 = 4$?

Answer: Since $2 \cdot 4 \equiv 1 \pmod{7}$, we can rewrite $4m \bmod 7 = 1$ as

$$2 \cdot 4m \bmod 7 = m \bmod 7 = 2 \cdot 1 \bmod 7 = 2.$$

Since $2 \cdot 3 \equiv 1 \pmod{5}$, we can rewrite $3m \bmod 5 = 4$ as

$$2 \cdot 3m \bmod 5 = m \bmod 5 = 2 \cdot 4 \bmod 5 = 3.$$

To solve $m \bmod 7 = 2$ and $m \bmod 5 = 3$ we use the Chinese Remainder Theorem to get $m = (2 \cdot 5 \cdot 3 + 3 \cdot 7 \cdot 3) \bmod 7 \cdot 5 = 23$.

Subtracting $7 \cdot 5 = 35$ to get the negative solution with smallest absolute value yields $m = -12$.

Question 2) (10 points) What $k < 0$ that is smallest in absolute value satisfies $2k \bmod 3 = 1$ and $5k \bmod 8 = 3$?

Answer: Since $2 \cdot 2 \equiv 1 \pmod{3}$, we can rewrite $2k \bmod 3 = 1$ as

$$2 \cdot 2k \bmod 3 = k \bmod 3 = 2 \cdot 1 \bmod 3 = 2.$$

Since $5 \cdot 5 \equiv 1 \pmod{8}$, we can rewrite $5k \bmod 8 = 3$ as

$$5 \cdot 5k \bmod 8 = k \bmod 8 = 5 \cdot 3 \bmod 8 = 7.$$

To solve $k \bmod 3 = 2$ and $k \bmod 8 = 7$ we use the Chinese Remainder Theorem to get $k = (2 \cdot 8 \cdot 2 + 7 \cdot 3 \cdot 3) \bmod 3 \cdot 8 = 23$.

Subtracting $3 \cdot 8 = 24$ to get the negative solution with smallest absolute value yields $k = -1$.

Question 3) (10 points) Consider the sequence defined by $A(0) = 1$, $A(1) = 2$, $A(n) = -3 \cdot A(n-2)$ for $n \geq 2$.

1. List $A(2)$ through $A(6)$

Answer: $A(2) = -3$, $A(3) = -6$, $A(4) = 9$, $A(5) = 18$, $A(6) = -27$.

2. Give a closed form formula for $A(n)$ for $n \geq 0$. It is acceptable if your formula has a small set of cases.

Answer: By inspection, we get the answer

$$A(n) = \begin{cases} (-3)^{n/2} & \text{if } n \text{ is even} \\ 2(-3)^{(n-1)/2} & \text{if } n \text{ is odd} \end{cases}$$

Alternatively, look for solutions of the form r^n , so $r^2 = -3$, or $r_{\pm} = \pm i\sqrt{3}$. The solution will be $A(n) = \alpha(i\sqrt{3})^n + \beta(-i\sqrt{3})^n$ for some α and β satisfying $1 = A(0) = \alpha + \beta$ and $2 = A(1) = \alpha r_+ + \beta r_-$, yielding $\alpha = .5 - i/\sqrt{3}$ and $\beta = .5 + i/\sqrt{3}$ and

$$A(n) = (.5 - i/\sqrt{3}) \cdot (i\sqrt{3})^n + (.5 + i/\sqrt{3}) \cdot (-i\sqrt{3})^n$$

Question 3) (10 points) Consider the sequence defined by $B(1) = 2$, $B(2) = 3$, $B(n) = -5 \cdot B(n-2)$ for $n \geq 3$.

1. List $B(3)$ through $B(7)$

Answer: $B(3) = -10$, $B(4) = -15$, $B(5) = 50$, $B(6) = 75$, $B(7) = -250$.

2. Give a closed form formula for $B(n)$ for $n \geq 1$. It is acceptable if your formula has a small set of cases.

Answer: By inspection, we get the answer

$$B(n) = \begin{cases} 3(-5)^{(n-2)/2} & \text{if } n \text{ is even} \\ 2(-5)^{(n-1)/2} & \text{if } n \text{ is odd} \end{cases}$$

Alternatively, look for solutions of the form r^n , so $r^2 = -5$, or $r_{\pm} = \pm i\sqrt{5}$. The solution will be $B(n) = \alpha(i\sqrt{5})^n + \beta(-i\sqrt{5})^n$ for some α and β satisfying $2 = B(1) = \alpha r_+ + \beta r_-$ and $3 = B(2) = \alpha r_+^2 + \beta r_-^2$, yielding $\alpha = -.3 - i/\sqrt{5}$ and $\beta = -.3 + i/\sqrt{5}$ and

$$B(n) = (-.3 - i/\sqrt{5}) \cdot (i\sqrt{5})^n + (-.3 + i/\sqrt{5}) \cdot (-i\sqrt{5})^n$$

Question 3) (10 points) Consider the sequence defined by $C(-1) = 2$, $C(0) = 1$, $C(n) = -7 \cdot C(n-2)$ for $n \geq 1$.

1. List $C(1)$ through $C(5)$

Answer: $C(1) = -14$, $C(2) = -7$, $C(3) = 98$, $C(4) = 49$, $C(5) = -686$.

2. Give a closed form formula for $C(n)$ for $n \geq -1$. It is acceptable if your formula has a small set of cases.

Answer: By inspection, we get the answer

$$C(n) = \begin{cases} (-7)^{n/2} & \text{if } n \text{ is even} \\ 2(-7)^{(n+1)/2} & \text{if } n \text{ is odd} \end{cases}$$

Alternatively, look for solutions of the form r^n , so $r^2 = -7$, or $r_{\pm} = \pm i\sqrt{7}$. The solution will be $C(n) = \alpha(i\sqrt{7})^n + \beta(-i\sqrt{7})^n$ for some α and β satisfying $2 = C(-1) = \alpha r_+^{-1} + \beta r_-^{-1}$ and $1 = C(0) = \alpha + \beta$, yielding $\alpha = .5 + i\sqrt{7}$ and $\beta = .5 - i\sqrt{7}$ and

$$C(n) = (.5 + i\sqrt{7}) \cdot (i\sqrt{7})^n + (.5 - i\sqrt{7}) \cdot (-i\sqrt{7})^n$$

Question 4) (10 points) Prove by induction that $12|(3^n + 7^n + 2)$ for $n \geq 1$. Note: you have to use induction.

Answer: Base case: When $n = 1$, $3^1 + 7^1 + 2 = 12$ and $12|12$.

Induction step: Assume $12|(3^n + 7^n + 2)$. Then

$$\begin{aligned}3^{n+1} + 7^{n+1} + 2 &= 3 \cdot 3^n + 7 \cdot 7^n + 2 \\ &= 7 \cdot 3^n + 7 \cdot 7^n + 7 \cdot 2 - 4 \cdot 3^n - 12 \\ &= 7 \cdot (3^n + 7^n + 2) - 4 \cdot 3^n - 12\end{aligned}$$

Now $12|7 \cdot (3^n + 7^n + 2)$ by the induction hypothesis. Clearly $12 = 4 \cdot 3|4 \cdot 3^n$, so 12 divides the sum $7 \cdot (3^n + 7^n + 2) - 4 \cdot 3^n - 12$ as desired.

Question 4) (10 points) Prove by induction that $10|(5^m + 6^m - 1)$ for $m \geq 1$. Note: you have to use induction.

Answer: Base case: When $m = 1$, $5^1 + 6^1 - 1 = 10$ and $10|10$.

Induction step: Assume $10|(5^m + 6^m - 1)$. Then

$$\begin{aligned}5^{m+1} + 6^{m+1} - 1 &= 5 \cdot 5^m + 6 \cdot 6^m - 1 \\&= 6 \cdot 5^m + 6 \cdot 6^m - 6 \cdot 1 - 5^m + 5 \\&= 6 \cdot (5^m + 6^m - 1) - 5 \cdot (5^{m-1} - 1)\end{aligned}$$

Now $10|6 \cdot (5^m + 6^m - 1)$ by the induction hypothesis. Since 5 is odd, so is 5^{m-1} , and so $5^{m-1} - 1$ is even, i.e. $2|(5^{m-1} - 1)$, so $10|5(5^{m-1} - 1)$. Thus 10 divides the difference $6 \cdot (5^m + 6^m - 1) - 5 \cdot (5^{m-1} - 1)$ as desired.

Question 4) (10 points) Prove by induction that $6|(3^k + 4^k + 5)$ for $k \geq 1$. Note: you have to use induction.

Answer: Base case: When $k = 1$, $3^1 + 4^1 + 5 = 12$ and $6|12$.

Induction step: Assume $6|(3^k + 4^k + 5)$. Then

$$\begin{aligned}3^{k+1} + 4^{k+1} + 5 &= 3 \cdot 3^k + 4 \cdot 4^k + 5 \\&= 4 \cdot 3^k + 4 \cdot 4^k + 4 \cdot 5 - 3^k - 15 \\&= 4 \cdot (3^k + 4^k + 5) - 3 \cdot (3^{k-1} - 5)\end{aligned}$$

Now $6|4 \cdot (3^k + 4^k + 5)$ by the induction hypothesis. Next, 3^{k-1} and 5 are odd so their difference is even, so $2|(3^{k-1} - 5)$, so $6|3(3^{k-1} - 5)$. Thus 6 divides the difference $4 \cdot (3^k + 4^k + 5) - 3 \cdot (3^{k-1} - 5)$ as desired.

Question 5 (10 points) This problem contains a true statement and a “proof” of that statement. You must

- say whether the proof is valid or invalid,
- if it is invalid, describe exactly on which line and how it *first* goes wrong, and
- if it is invalid, how can you fix it.

Statement: “Let $m > 1$ be an integer. Let $\phi(m)$ be the number of integers between 1 and m that are relatively prime to m . Suppose $\gcd(a, m) = 1$. Then $a^{\phi(m)} \equiv 1 \pmod{m}$.”

Here is the “proof” (with line numbers added for your convenience in referring to them.)

1. Let $1 = n_1 < n_2 < \cdots < n_{\phi(m)} = m - 1$ be the list of $\phi(m)$ integers between 1 and m that are relatively prime to m .
2. Since $\gcd(n_i, m) = 1$, there is a unique inverse x_i of $n_i \pmod{m}$, i.e. a unique x_i that satisfies $x_i \cdot n_i \equiv 1 \pmod{m}$.
3. $x_1 = n_1 = 1$ and $x_{\phi(m)} = n_{\phi(m)} = m - 1$.
4. The only solutions of $n^2 \equiv 1 \pmod{m}$ are $n = 1$ and $n = m - 1$.
5. The other n_i besides n_1 and $n_{\phi(m)}$ can be grouped into pairs (n_i, n_j) such that $i \neq j$ and $n_i n_j \equiv 1 \pmod{m}$ i.e. n_i and n_j are inverses of one another.
6. The product $n_1 \cdot n_2 \cdots n_{\phi(m)} \equiv -1 \pmod{m}$.
7. The products $a \cdot n_1, \dots, a \cdot n_{\phi(m)}$ are all relatively prime to m .
8. The products $a \cdot n_1, \dots, a \cdot n_{\phi(m)}$ are all different \pmod{m} , i.e. $a \cdot n_i \not\equiv a \cdot n_j \pmod{m}$ if $i \neq j$.
9. The products $a \cdot n_1 \pmod{m}, \dots, a \cdot n_{\phi(m)} \pmod{m}$ are the same as $n_1, \dots, n_{\phi(m)}$, perhaps in a different order.
10. $(a \cdot n_1 \pmod{m}) \cdots (a \cdot n_{\phi(m)} \pmod{m}) \equiv n_1 \cdots n_{\phi(m)} \pmod{m}$.
11. $-a^{\phi(m)} \equiv -1 \pmod{m}$, by line 6.
12. $a^{\phi(m)} \equiv 1 \pmod{m}$, as desired.

Answer: The theorem is true, but the proof is invalid, unless m is a prime, in which case $\phi(m) = m - 1$ and the result is called Fermat’s Little Theorem. The flaw is in line 4. For example, consider $m = 8$. Then $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1$. The correct proof observes that line 10 is still valid. Then we can “cancel” $\prod_{i=1}^{\phi(m)} n_i$ out \pmod{m} since it is relatively prime to m .

Question 5 (10 points) This problem contains a true statement and a “proof” of that statement. You must

- say whether the proof is valid or invalid,
- if it is invalid, describe exactly on which line and how it *first* goes wrong, and
- if it is invalid, how can you fix it.

Statement: “Let $n > 1$ be an integer. Let $\rho(n)$ be the number of integers i between 1 and n satisfying $\gcd(i, n) = 1$. Suppose also $\gcd(b, n) = 1$. Then $b^{\rho(n)} \equiv 1 \pmod{n}$.”

Here is the “proof” (with line numbers added for your convenience in referring to them.)

1. Let $1 = m_1 < m_2 < \cdots < m_{\rho(n)} = n - 1$ be the list of $\rho(n)$ integers between 1 and n that are relatively prime to n .
2. Since $\gcd(m_j, n) = 1$, there is a unique inverse y_j of $m_j \pmod{n}$, i.e. a unique y_j that satisfies $y_j \cdot m_j \equiv 1 \pmod{n}$.
3. $y_1 = m_1 = 1$ and $y_{\rho(n)} = m_{\rho(n)} = n - 1$.
4. The only solutions of $m^2 \equiv 1 \pmod{n}$ are $m = 1$ and $m = n - 1$.
5. The other m_j besides m_1 and $m_{\rho(n)}$ can be grouped into pairs (m_k, m_j) such that $k \neq j$ and $m_k m_j \equiv 1 \pmod{n}$ i.e. m_k and m_j are inverses of one another.
6. The product $m_1 \cdot m_2 \cdots m_{\rho(n)} \equiv -1 \pmod{n}$.
7. The products $b \cdot m_1, \dots, b \cdot m_{\rho(n)}$ are all relatively prime to n .
8. The products $b \cdot m_1, \dots, b \cdot m_{\rho(n)}$ are all different \pmod{n} , i.e. $b \cdot m_k \not\equiv b \cdot m_j \pmod{n}$ if $k \neq j$.
9. The products $b \cdot m_1 \pmod{n}, \dots, b \cdot m_{\rho(n)} \pmod{n}$ are the same as $m_1, \dots, m_{\rho(n)}$, perhaps in a different order.
10. $(b \cdot m_1 \pmod{n}) \cdots (b \cdot m_{\rho(n)} \pmod{n}) \equiv m_1 \cdots m_{\rho(n)} \pmod{n}$.
11. $-b^{\rho(n)} \equiv -1 \pmod{n}$, by line 6.
12. $b^{\rho(n)} \equiv 1 \pmod{n}$, as desired.

Answer: The theorem is true, but the proof is invalid, unless n is a prime, in which case $\rho(n) = n - 1$ and the result is called Fermat’s Little Theorem. The flaw is in line 4. For example, consider $n = 8$. Then $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1$. The correct proof observes line 10 is still valid. Then we can “cancel” $\prod_{i=1}^{\rho(n)} m_i$ out \pmod{n} , since it is relatively prime to n .

Question 5) (10 points) This problem contains a true statement and a “proof” of that statement. You must

- say whether the proof is valid or invalid,
- if it is invalid, describe exactly on which line and how it *first* goes wrong, and
- if it is invalid, how can you fix it.

Statement: “Let $k > 1$ be an integer. Let $\omega(k)$ be the number of integers j between 1 and k satisfying $\gcd(j, k) = 1$. Suppose also c and k are relatively prime. Then $c^{\omega(k)} \equiv 1 \pmod{k}$.”

Here is the “proof” (with line numbers added for your convenience in referring to them.)

1. Let $1 = r_1 < r_2 < \dots < r_{\omega(k)} = k - 1$ be the list of $\omega(k)$ integers between 1 and k that are relatively prime to k .
2. Since $\gcd(r_i, k) = 1$, there is a unique inverse z_i of $r_i \pmod{k}$, i.e. a unique z_i that satisfies $z_i \cdot r_i \equiv 1 \pmod{k}$.
3. $z_1 = r_1 = 1$ and $z_{\omega(k)} = r_{\omega(k)} = k - 1$.
4. The only solutions of $r^2 \equiv 1 \pmod{k}$ are $r = 1$ and $r = k - 1$.
5. The other r_i besides r_1 and $r_{\omega(k)}$ can be grouped into pairs (r_i, r_j) such that $i \neq j$ and $r_i r_j \equiv 1 \pmod{k}$ i.e. r_i and r_j are inverses of one another.
6. The product $r_1 \cdot r_2 \cdot \dots \cdot r_{\omega(k)} \equiv -1 \pmod{k}$.
7. The products $c \cdot r_1, \dots, c \cdot r_{\omega(k)}$ are all relatively prime to k .
8. The products $c \cdot r_1, \dots, c \cdot r_{\omega(k)}$ are all different \pmod{k} , i.e. $c \cdot r_i \not\equiv c \cdot r_j \pmod{k}$ if $i \neq j$.
9. The products $c \cdot r_1 \pmod{k}, \dots, c \cdot r_{\omega(k)} \pmod{k}$ are the same as $r_1, \dots, r_{\omega(k)}$, perhaps in a different order.
10. $(c \cdot r_1 \pmod{k}) \cdot \dots \cdot (c \cdot r_{\omega(k)} \pmod{k}) \equiv r_1 \cdot \dots \cdot r_{\omega(k)} \pmod{k}$.
11. $-c^{\omega(k)} \equiv -1 \pmod{k}$, by line 6.
12. $c^{\omega(k)} \equiv 1 \pmod{k}$, as desired.

Answer: The theorem is true, but the proof is invalid, unless k is a prime, in which case $\omega(k) = k - 1$ and the result is called Fermat’s Little Theorem. The flaw is in line 4. For example, consider $k = 8$. Then $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1$. The correct proof observes line 10 is still valid. Then we can “cancel” $\prod_{i=1}^{\omega(k)} r_i$ out \pmod{k} , since it is relatively prime to k .