1. For each of the following statements, write its negation and its contrapositive.
   a) If $2 \nmid x$, then $2|(x+1)$.
   Negation: $2 \nmid x$ and $2 \nmid (x+1)$
   Contrapositive: If $2 \nmid (x+1)$, then $2|x$.
   b) If an integer p is prime, then either $2^p - 1$ is prime or p is divisible by 3.
   Negation: An integer p is prime, and $2^p - 1$ is not prime and p is not divisible by 3.
   Contrapositive: For an integer p, if $2^p - 1$ is not prime and p is not divisible by 3, then p is not prime.
   c) Let a and b be integers. If $a(b^2 - 2b)$ is odd, then a and b are both odd.
   Negation: Let a and b be integers, we have $a(b^2 - 2b)$ is odd and at least one of a and b is even.
   Contrapositive: Let a and b be integers. If at least one of a and b is even, then $a(b^2 - 2b)$ is even.
   (Note: We have used the basic proposition that if an integer is not odd, then it is even.)
   d) For all integers a, b, c, if $a|b$ and $b|c$, then $a|c$.
   Negation: For all integers a, b, c, we have $a|b$ and $b|c$, and $a \nmid c$.
   Contrapostitive: For all integers a, b, c, if $a \nmid c$, then $a \nmid b$ or $b \nmid c$.
2. Show that $(\neg p) \wedge \big(q \vee (\neg p)\big)$ is logically equivalent to $p \to \big(\neg(q \vee p)\big)$.

p	q	$\neg p$	$q \vee (\neg p)$	$(\neg p) \wedge \big(q \vee (\neg p)\big)$	$q \vee p$	$\neg(q \vee p)$	$p \to \big(\neg(q \vee p)\big)$
T	T	F	T	F	T	F	F
T	F	F	F	F	T	F	F
F	T	T	T	T	T	F	T
F	F	T	T	T	F	T	T

3. Prove that for all integers a, b, c, if $a|b$ and $b|c$, then $a|c$.
If $a|b$ and $b|c$, then $b = an$ and $c = bm$ for some integers n and m. So, $c = bm = anm = a(nm)$, where nm is an integer. Hence, $a|c$.
4. Prove that there are no integers a and b such that $3a - 9b = 2$.
Suppose there were integers a and b such that $3a - 9b = 2$, then $3a - 9b = 3(a - 3b) = 2$, and $3|2$, which is not true!
5. Prove the following proposition:
   If a and b are real numbers and $a + b = 0$, then $a \le 0$ or $b \le 0$.
We may prove by contradiction:
   Suppose $a > 0$ and $b > 0$, then $a + b > 0$, contradicting the given fact that $a + b = 0$.
We may prove by contrapositve:
   The contrapositive of the proposition is: If a and b are positive real numbers, then $a + b \neq 0$.
   Proof of the contrapositive: If $a > 0$ and $b > 0$, then $a + b > 0$, and $a + b \neq 0$.
6. Prove the following proposition by contrapositive.
   Let a be a positive integer. If $a \equiv 2\ (mod\ 4)$ or $a \equiv 3\ (mod\ 4)$, then a is not a perfect square.
The contrapositive is:
   Let a be a positive integer. If a is a perfect square, then $a \not\equiv 2\ (mod\ 4)$ and $a \not\equiv 3\ (mod\ 4)$, in other words, $a \equiv 0\ (mod\ 4)$ or $a \equiv 1\ (mod\ 4)$.
Proof of the contrapositive: Note that an integer is odd or even.
   If a is the square of an even integer, then $a = (2n)^2$ for some integer n and $a = 4n^2$, where n^2 is an integer, and so $a \equiv 0\ (mod\ 4)$.
   If a is the square of an odd integer, then $a = (2n+1)^2$ for some integer n and
   $$a = 4n^2 + 4n + 1 = 4(n^2 + n) + 1$$
   where $n^2 + n$ is an integer, and $a \equiv 1\ (mod\ 4)$.
7. Prove that for all prime p, $\sqrt{p}$ is irrational. You may use the following proposition:
   Proposition: For any prime p and integers a, b, if $p|ab$, $p|a$ or $p|b$.
We prove by contradiction. Suppose that $\sqrt{p}$ is rational, then it can be written as an irreducible fraction of integers, i.e. $\sqrt{p} = m/n$, where m and n do not have a common factor/divisor (other than 1 or -1).

It follows that $m^2/n^2 = p$, which implies that $m^2 = pn^2$. Since n^2 is an integer, we have $p|m^2$. By the given proposition, we have $p|m$, and we may write $m = pk$ for some integer k. Then $m^2 = p^2k^2$. Earlier, we have $m^2 = pn^2$, so $pn^2 = p^2k^2$, which implies that $n^2 = pk^2$. Since k^2 is an integer, we have $p|n^2$ and $p|n$. We have shown that both m and n are divisible by p, contradicting the fact that m/n is irreducible!

8. Given the sets,

$$A = \{1,2,3,4,5\}, \quad B = \{x \in A: x \text{ is prime}\}, \quad C = \{x \in A: x \text{ is odd}\},$$
$$D = \{x \in A: 2|x\}, \quad E = \{x \in A: x|2\}$$

We first list B, C, D, and E:

$$B = \{2,3,5\}, \quad C = \{1,3,5\}, \quad D = \{2,4\}, \quad E = \{1,2\}$$

List the elements of:

a) $A - (B \cap C)$

$$B \cap C = \{3,5\}, \quad A - (B \cap C) = \{1,2,4,\}$$

b) $(A - B) \cap (A - C)$

$$A - B = \{1,4\}, \quad A - C = \{1,3,5\}, \quad (A - B) \cap (A - C) = \{1\}$$

c) $A - (D \cup E)$

$$D \cup E = \{1,2,4\}, \quad A - (D \cup E) = \{3,5\}$$

d) $(A - D) \cup (A - E)$

$$A - D = \{1,3,5\}, \quad A - E = \{3,4,5\}, \quad (A - D) \cup (A - E) = \{1,3,4,5\}$$

e) $(B - C) \times (C - B)$

$$B - C = \{2\}, \quad C - B = \{1\}, \quad (B - C) \times (C - B) = \{(2,1)\}$$

f) $B\Delta C$

$$B\Delta C = (B - C) \cup (C - B) = \{1,2\}$$

g) $2^{B \cap C}$

$$B \cap C = \{3,5\}, \quad 2^{B \cap C} = \{\emptyset, \{3\}, \{5\}, \{3,5\}\}$$

h) $2^B \cap 2^C$

$$2^B \cap 2^C = \{X : X \subseteq B \text{ and } X \subseteq C\} = \{\emptyset, \{3\}, \{5\}, \{3,5\}\}$$

Note that we can prove that for any sets S and T, $2^{S \cap T} = 2^S \cap 2^T$: $X \in 2^S \cap 2^T$ if and only if $X \subseteq S$ and $X \subseteq T$, which is true if and only if to $X \subseteq (S \cap T)$, which is equivalent to $2^{S \cap T}$.

j) $2^{D \cup E}$

$$D \cup E = \{1,2,4\}, \quad 2^{D \cup E} = \{\emptyset, \{1\}, \{2\}, \{4\}, \{1,2\}, \{1,4\}, \{2,4\}, \{1,2,4\}\}$$

k) $2^D \cup 2^E$

$$2^D \cup 2^E = \{X : X \subseteq D \text{ or } X \subseteq E\} = \{\emptyset, \{1\}, \{2\}, \{4\}, \{1,2\}, \{2,4\}\}$$

Note that $2^{D \cup E} \neq 2^D \cup 2^E$. One can prove that for any sets S and T, if $S \nsubseteq T$ and $T \nsubseteq S$, then $2^{S \cup T} \neq 2^S \cup 2^T$: Suppose $S \nsubseteq T$ and $T \nsubseteq S$, then there is an element $x \in S \cup T$ such that $x \notin S$ and there is an element $y \in S \cup T$ such that $y \notin T$. So $X = \{x, y\}$ is a subset of $S \cup T$, that is, $X \in 2^{S \cup T}$, but X is neither a subset of S nor a subset of T, that is, $X \notin 2^S \cup 2^T$. Hence, $2^{S \cup T} \neq 2^S \cup 2^T$.

9. Prove or disprove the following statement:

Let A, B, C be sets. If $A - B = A - C$, then $B = C$.

We can disprove with a counterexample:

Let $A = \{1,2\}, B = \{1,3\}$, and $C = \{1,4\}$, then $A - B = A - C = \{1\}$ but $B \neq C$.

10. Let $A = \{x + 3y: x, y \in \mathbb{Z}\}$ and B be the set of all even integers. Prove or disprove:

a) $A \subseteq B$

We disprove by a counterexample: We have $2 + 3(1) = 5 \in A$ but $5 \notin B$.

b) $B \subseteq A$

Proof: Let $b \in B$, then $b = 2m$ for some integer m, and $b = 2m = -m + 3m = x + y$, where $x = -m$ and $y = m$ are both integers, so $b \in A$.

11. Prove or disprove the following statement:

Let p, q be distinct primes. Suppose A is the set of multiples of p, B is the set of multiples of q, C is the set of multiples of pq, then $C = A \cap B$.

You may use the following proposition:

Proposition: For any prime p and integers a, b, if $p|ab$, then $p|a$ or $p|b$.

Proof: Let $x \in C$, then $x = pqn$ for some integer n, and $x = p(qn) = pk$ and $x = q(pn) = ql$, where k and l are integers. So, $x \in A$ and $x \in B$, that is, $x \in A \cap B$. We have proved that $C \subseteq A \cap B$. Next, let $x \in A \cap B$, then $x = pn$ and $x = qm$ for some integers n, m. So, $x = pn = qm$, and $p|qm$. According to the given proposition, since p does not divide q, it must divides m. Therefore

$$x = qm = q(pk) = (pq)k$$

for some integer k, and $pq|x$, and $x \in C$.

12. Let $A = \{1,2,3,4\}$, and consider the relation on A defined by

$$R = \{(1,1), (2,1), (3,1), (4,1), (2,3), (4,4)\}$$

Prove or disprove the following.

a) R is a function.
R is NOT a function because $(2,1) \in R$ and $(2,3) \in R$, but $1 \neq 3$.

b) R is reflexive.
R is NOT reflexive because $2 \in A$ but $(2,2) \notin R$.

c) R is irreflexive.
R is NOT irreflexive because $(1,1) \in R$.

d) R is symmetric.
R is NOT symmetric because $(2,1) \in R$ but $(1,2) \notin R$.

e) R is antisymmetric.
R is antisymmetric because whenever $(x, y) \in R$ and $(y, x) \in R$ (only true when $x = y = 1$), we have $x = y$.

f) R is transitive.
R is transitive because whenever $(x, y) \in R$ and $(y, z) \in R$, we have $(x, z) \in R$.

g) R is an equivalence relation.
R is not an equivalence relation since R is not reflexive (or since R is not symmetric).

13. Let $A = \{1,2,3,4\}$ and R be a relation on A.

a) Find the smallest R which is reflexive.

$$R = \{(1,1), (2,2), (3,3), (4,4)\}$$

b) Find the smallest R which is irreflexive.
The smallest set that does not include any of (x, x) is the set that does not include anything: $\emptyset$!

c) Explain why there is NO relation R which is both reflexive and irreflexive. Can a relation (on any set) ever be both reflexive and irreflexive?
If R is reflexive, it must include $(1,1)$, but then it is not irreflexive. A relation can be both reflexive and irreflexive only if it is a relation on an empty set, whereby the only relation is $\emptyset$, which is both reflexive and irreflexive.

d) Find a relation R which is neither reflexive nor irreflexive.

$$R = \{(1,1)\}$$

e) Find a relation R which is reflexive and symmetric but not transitive.

$$R = \{(1,1), (2,2), (3,3), (4,4), (1,2), (2,1), (2,3), (3,2)\}$$

f) Find a relation R which is reflexive and transitive but not symmetric.
A smallest example is $R = \{(1,1), (2,2), (3,3), (4,4), (1,2)\}$, a bigger example is

$$R = \{(1,1), (2,2), (3,3), (4,4), (1,2), (2,3), (1,3)\}$$

g) Find a relation R which is symmetric and transitive but not reflexive.
A smallest example is $R = \{(1,1)\}$, a bigger example is $R = \{(1,1), (1,2), (2,1), (2,2)\}$.

h) Let R be a relation on A defined by $R = \{(1,1), (1,2), (1,3)\}$. Find the smallest relation S on A such that $R \subset S$ and S is symmetric.

$$R = \{(1,1), (1,2), (1,3), (2,1), (3,1)\}$$

i) Let R be a relation on A defined by $R = \{(1,4),(4,1)\}$. Find the smallest relation S on A such that $R \subset S$ and S is transitive.

$$R = \{(1,1),(4,4),(1,4),(4,1)\}$$

14. Let A be a finite set and let R be a relation on A. Prove the following.

a) $(R^{-1})^{-1} = R$

To show that $(R^{-1})^{-1} = R$, we will show that $(R^{-1})^{-1} \subseteq R$ and $R \subseteq (R^{-1})^{-1}$.

Let $(a,b) \in (R^{-1})^{-1}$. Then $(b,a) \in R^{-1}$, and $(a,b) \in R$. We have shown that $(R^{-1})^{-1} \subseteq R$.

Let $x = (a,b) \in R$. Then $(b,a) \in R^{-1}$, and $(a,b) \in (R^{-1})^{-1}$. So $R \subseteq (R^{-1})^{-1}$.

b) $R = R^{-1}$ if and only if R is symmetric.

($\Rightarrow$) Let $(x,y) \in R$. Since $R = R^{-1}$, we have $(x,y) \in R^{-1}$, which implies that $(y,x) \in R$, so R is symmetric.

($\Leftarrow$) We show that $R = R^{-1}$ by showing that $R \subseteq R^{-1}$ and $R^{-1} \subseteq R$. Let $(x,y) \in R$. Since R is symmetric, $(y,x) \in R$. This implies that $(x,y) \in R^{-1}$. So, $R \subseteq R^{-1}$. Next, let $(x,y) \in R^{-1}$. Then $(y,x) \in (R^{-1})^{-1} = R$. Since R is symmetric, $(x,y) \in R$, so $R^{-1} \subseteq R$.

15. Suppose R is an equivalence relation on a set A. Show that:

For every $a, b \in A$, $a \in [b] \iff b \in [a]$.

($\Rightarrow$) Suppose $a \in [b]$, then aRb by definition. Since R is symmetric (because it is an equivalence relation), we have bRa, so $b \in [a]$.

Exactly the same argument goes in ($\Leftarrow$), we just interchange a and b.

16. For each of the following, explain why it is NOT an equivalence relation.

a) "$\subseteq$", i.e. inclusion on sets

It is not symmetric: $\{1\} \subseteq \{1,2\}$ but $\{1,2\} \nsubseteq \{1\}$.

b) "$|$", i.e. divides on integers

It is not symmetric: $1|2$ but $2 \nmid 1$.

c) R is a relation on $\mathbb{Z}$, and $R = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : y = 2x\}$

It is not reflexive: $(1,1) \notin R$ because $1 \neq 2(1)$.

d) R is a relation on $\mathbb{Z}$, and $R = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : x - y \geq 0\}$

It is not symmetric: $(1,0) \in R$ (because $1 - 0 \geq 0$), but $(0,1) \notin R$ (because $0 - 1 \ngeq 1$).

e) R is a relation on $\{a,b,c\}$, and $R = \{(a,a),(b,b),(c,c),(a,c),(c,a),(b,c),(c,b)\}$

It is not transitive: $(a,c) \in R$ and $(c,b) \in R$, but $(a,b) \notin R$.

17. Let $A = \{0,1,2,\dots,10\}$ and $R = \{(a,b) \in A \times A : 2|(a+b)\}$.

a) Show that R is an equivalence relation.

- R is reflexive: Let $a \in A$, we have $(a,a) \in R$ because $a + a = 2a$ and $2|(a+a)$.
- R is symmetric: If $(a,b) \in R$, then $2|(a+b)$. Since $b + a = a + b$, we have $2|(b+a)$ and $(b,a) \in R$.
- R is transitive: If $(a,b) \in R$ and $(b,c) \in R$, then $2|(a+b)$ and $2|(b+c)$. Therefore $a + b = 2n$ and $b + c = 2m$ for some integers n and m. So,

$$a + c = (2n - b) + (2m - b) = 2(n + m - b)$$

and $2|(a+c)$, that is, $(a,c) \in R$.

b) Compute the distinct equivalence classes of R.

$$[0] = \{x \in A : 2|(0+x)\} = \{x \in A : 2|x\} = \{0,2,4,6,8,10\}$$

$$[1] = \{x \in A : 2|(1+x)\} = \{x \in A : x + 1 = 2n \text{ for some integer } n\}$$
$$= \{x \in A : x = 2(n-1) + 1 \text{ for some integer } n\} = \{x \in A : x \text{ is odd}\}$$
$$= \{1,3,5,7,9\}$$

18. Let $R = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} : x^2 = y^2\}$.

a) Show that R is an equivalence relation.

- R is reflexive: Let $x \in A$, we have $(x,x) \in R$ because $x^2 = x^2$.
- R is symmetric: If $(x,y) \in R$, then $x^2 = y^2$, which implies that $y^2 = x^2$, so $(y,x) \in R$.
- R is transitive: If $(x,y) \in R$ and $(y,z) \in R$, then $x^2 = y^2 = z^2$, so $(x,z) \in R$.

b) Compute the distinct equivalence classes of R.
There are infinitely many distinct equivalence classes:
$$[0] = \{0\}, \quad [1] = \{-1,1\}, \quad [2] = \{-2,2\}, \quad [3] = \{-3,3\}, \quad \ldots.$$

19. What are all possible equivalence relations on $A = \{1,2,3\}$?
The smallest equivalence relation is $R_1 = \{(1,1),(2,2),(3,3)\}$. Next we must add at least a pair: (x,y) and (y,x), where $x \neq y$. So the next 3 equivalence relations are
$$R_2 = R_1 \cup \{(1,2),(2,1)\}, \quad R_3 = R_1 \cup \{(1,3),(3,1)\}, \quad R_4 = R_1 \cup \{(2,3),(3,2)\}$$
If we add an element to R_2, R_3, or R_4, we must add all elements in $A \times A$ to satisfy symmetry and transitivity, so the final equivalence relation is $R_5 = A \times A$.
Another, and a very good way to think about this question, is to make use of the fact that every equivalence relation on A defines a partition on A and vice versa. So, the question becomes, how many partitions are possible on A, that is, how many ways are there to divide A into disjoint subsets whose union is A? (These disjoint subsets are equivalence classes.) We can list them all:
- $\{1,2,3\}$
- $\{1,2\},\{3\}$
- $\{1,3\},\{2\}$
- $\{2,3\},\{1\}$
- $\{1\},\{2\},\{3\}$

20. For each of the following functions, determine if it is one-to-one, onto, or both. Prove your assertions.
a) $f: \mathbb{Z} \to \mathbb{Z}$ defined by
$$f(x) = \begin{cases} \dfrac{x}{2} & \text{if } x \text{ is even} \\ \dfrac{x+1}{2} & \text{if } x \text{ is odd} \end{cases}$$
- f is NOT one-to-one: $f(1) = f(2) = 1$.
- f is onto: Let $y \in \mathbb{Z}$ (codomain). Then $2y$ is even, $2y \in \mathbb{Z}$ (domain), and
$$f(2y) = 2y/2 = y$$

b) $g: \mathbb{N} \times \mathbb{N} \to \mathbb{Z}$ defined by $g(n,m) = n - m$
- g is NOT one-to-one: $f(1,0) = f(2,1) = 1$.
- g is onto: Let $y \in \mathbb{Z}$. If $y \geq 0$, then $(y,0) \in \mathbb{N} \times \mathbb{N}$ and $f(y,0) = y$ y. If $y < 0$, then $(0,-y) \in \mathbb{N} \times \mathbb{N}$ and $f(0,-x) = 0 - (-x) = x$.

c) $h: \mathbb{N} \times \{0,1\} \to \mathbb{Z}$ defined by $h(x,y) = \begin{cases} 2x & \text{if } y = 0 \\ 2x+1 & \text{if } y = 1 \end{cases}$
- h is one-to-one: Suppose that $f(x_1,y_1) = f(x_2,y_2) = z$.
If z is even, then $f(x_1,y_1) = z$ implies that $z = 2x_1$ and $y_1 = 0$,
and $f(x_1,y_1) = z$ implies that $z = 2x_2$ and $y_2 = 0$.
So, $x_1 = x_2$ and $y_1 = y_2$, or $(x_1,y_1) = (x_2,y_2)$.
If z is odd, then $f(x_1,y_1) = z$ implies that $z = 2x_1 + 1$ and $y_1 = 1$,
and $f(x_1,y_1) = z$ implies that $z = 2x_2 + 1$ and $y_2 = 1$.
So, $x_1 = x_2$ and $y_1 = y_2$, or $(x_1,y_1) = (x_2,y_2)$.
- g is not onto. $f(x,y)$ is non-negative since we have $x \geq 0$, which implies $2x \geq 0$ and $2x + 1 \geq 0$. Therefore there is no (x,y) such that $f(x,y) = -1$.

21. Let A, B, C be sets, and suppose $f: A \to B$ and $g: B \to C$. Prove the following.
a) If f and g are one-to-one, then $g \circ f$ is one-to-one.
Suppose $(g \circ f)(x) = (g \circ f)(y)$, that is, $g(f(x)) = g(f(y))$.
Since g is one-to-one, we have $f(x) = f(y)$.
Since f is one-to-one, we have $x = y$.
So, $g \circ f$ is one-to-one.
b) If f and g are onto, then $g \circ f$ is onto.
Let $z \in C$.
Since g is onto, there exists $y \in B$ such that $g(y) = z$.

Since f is onto, there exists $x \in A$ such that $f(x) = y$.
So, there exists $x \in A$ such that $(g \circ f)(x) = g\big(f(x)\big) = g(y) = z$, that is, $g \circ f$ is onto.

c) If $g \circ f$ is one-to-one, then f is one-to-one. (Hint: Use contrapositive.)
Contrapositve: If f is not one-to-one, then $g \circ f$ is not one-to-one.
Proof of the contrapositive: If f is not one-to-one, then there exist $x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$. So, $(g \circ f)(x) = g\big(f(x)\big) = g\big(f(y)\big) = (g \circ f)(y)$, and $g \circ f$ is not one-to-one.

d) If $g \circ f$ is onto, then g is onto. (Hint: Use contrapositive.)
Contrapositve: If g is not onto, then $g \circ f$ is not onto.
Proof of the contrapositive: If g is not onto, then there exist $z \in C$ such that $g(y) \neq z$ for any $y \in B$. Let $x \in A$, then $f(x) \in B$. So $(g \circ f)(x) = g\big(f(x)\big) \neq z$, and $g \circ f$ is not onto.

22. Give a combinatorial interpretation of the identity $2^n 2^m = 2^{n+m}$ for all $n, m \in \mathbb{N}$.
Consider binary sequences of length $n + m$. There are $2 \times 2 \times \cdots \times 2 = 2^{n+m}$ such sequences. On the other hand, we may construct such a sequence by appending a binary sequence of length m (there are 2^m such sequences) to a binary sequence of length n (there are 2^n such sequences), so there are $2^n 2^m$ sequences.

23. Consider the identity
$$k!\binom{n}{k} = n(n-1)\cdots(n-k+1)$$

a) Prove this identity algebraically.
$$k!\binom{n}{k} = k!\frac{n!}{k!\,(n-k)!} = \frac{n!}{(n-k)!} = \frac{n(n-1)(n-2)\cdots(n-k+1)(n-k)(n-k-1)\cdots 3\cdot 2\cdot 1}{(n-k)(n-k-1)\cdots 3\cdot 2\cdot 1}$$
$$= n(n-1)\cdots(n-k+1)$$

b) Prove this identity combinatorially.
Consider the following question: How many ways are there to arrange k out of a family of n members in a row of chairs? There are two ways to answer this question.

- We may choose one of the n persons for the first chair. After the first person is chosen, there are $n-1$ persons to be chosen for the second chair, then there are $n-2$ persons for the third chair, etc, until are there $n-(k-1) = n-k+1$ choices for the kth chair. By the multiplication principle, the answer to the question is the RHS:
$$n(n-1)(n-2)\cdots(n-k+1)$$
- We may first choose k people from n people without arranging them, and there are $\binom{n}{k}$ ways of doing so. Next we arrange the chosen k people on the chairs, and there are $k(k-1)(k-2)\cdots 3\cdot 2\cdot 1 = k!$ ways to do this. Therefore the answer is the LHS:
$$\binom{n}{k}k!$$

24. Consider the identity
$$\binom{n}{r}\binom{r}{k} = \binom{n}{k}\binom{n-k}{r-k}$$

a) Prove this identity algebraically.
$$\binom{n}{k}\binom{n-k}{r-k} = \frac{n!}{k!\,(n-k)!}\frac{(n-k)!}{(r-k)!\big((n-k)-(r-k)\big)!} = \frac{n!}{k!\,(r-k)!\,(n-r)!}$$
$$= \frac{n!}{k!\,(r-k)!\,(n-r)!}\frac{r!}{r!} = \frac{n!}{r!\,(n-r)!}\frac{r!}{k!\,(r-k)!} = \binom{n}{r}\binom{r}{k}$$

b) Prove this identity combinatorially.
Suppose we want to choose a committee of r members from n people and a subcommittee of k members among the r committee members. We can choose the committee first and then the subcommittee, the number of ways to do this is given by the LHS: $\binom{n}{r}\binom{r}{k}$. We can also choose the subcommittee first, and then choose the rest of the committee from the rest of the people, the number of ways to do this is given by the RHS: $\binom{n}{k}\binom{n-k}{r-k}$.

25. Consider the identity

$$\binom{n}{k}\binom{n-k}{l} = \binom{n}{k+l}\binom{k+l}{l}$$

where n, k, l are non-negative integers and $n \geq k + l$.

a) Prove this identity algebraically.

$$\binom{n}{k+l}\binom{k+l}{l} = \frac{n!}{(k+l)!\,(n-k-l)!}\frac{(k+l)!}{l!\,k!} = \frac{n!}{l!\,k!\,(n-k-l)!}$$
$$= \frac{n!}{l!\,k!\,(n-k-l)!}\frac{(n-k)!}{(n-k)!} = \frac{n!}{k!\,(n-k)!}\frac{(n-k)!}{l!\,(n-k-l)!} = \binom{n}{k}\binom{n-k}{l}$$

b) Prove this identity combinatorially.

Suppose we have an n-element set. There are two ways to choose two disjoint subsets, one with k elements and one with l elements.

- The first way yields the LHS: We choose k elements from the whole set for the first subset, and then choose l elements from the remaining $n-k$ elements to form the second subset.
- The second way yields the RHS: We first choose all $k+l$ elements from the whole set, and then choose l elements to form one subset (and the k elements left will form the other subset).

26. A long shelf on a math professor's library wall holds 28 books, all of them in the fields of algebra, calculus, or discrete math. Prove that there must be at least 10 books in one of these 3 areas.

Suppose that there are at most 9 books in each area, then there would be at most 27 books in the shelf.

27. A donut shop sells 9 varieties of donut. On a certain day 92 people buy at least one donut. What is the minimum number of donuts that must have been purchased for at least one of the varieties?

Spread out 92 donuts as evenly as possible: $92 = 9(10) + 2$, so at least one variety has 11 donuts sold.

28. Let $A = \{a, b, c\}$ and $B = \{a, e, i, o, u\}$.

a) How many relations are there from A to B?

A relation from A to B is a subset of $A \times B$. Since $A \times B$ has $|A||B| = 3(5) = 15$ elements, $A \times B$ has 2^{15} subsets, and there are 2^{15} relations from A to B.

b) How many relations are there from B to A?

$$2^{|B\times A|} = 2^{5(3)} = 2^{15}$$

c) How many functions are there from A to B?

$$|B|^{|A|} = 5^3$$

d) How many functions are there from B to A?

$$|A|^{|B|} = 3^5$$

e) How many one-to-one functions are there from A to B?

$$5 \times 4 \times 3 = (5)_3$$

f) How many one-to-one functions are there from B to A?

Since there are more elements in B than in A, it is not possible for every element in B to be mapped to a different element in A, so there are 0 one-to-one functions from B to A.

29. Prove that for every integer n,

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$$

Basis step: check for $n = 1$,

$$\frac{1}{1\cdot 2} = 1 - \frac{1}{2}$$

Inductive step: Assume statement is true for $n = k$, that is,

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{k(k+1)} = 1 - \frac{1}{k+1}$$

Then for $n = k + 1$,

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{k(k+1)}+\frac{1}{(k+1)(k+2)}=1-\frac{1}{k+1}+\frac{1}{(k+1)(k+2)}$$
$$=1-\frac{1}{(k+1)(k+2)}(k+2-1)=1-\frac{1}{(k+1)(k+2)}(k+1)=1-\frac{1}{(k+2)}$$
The statement is true for $n=k+1$, and by induction, the statement is true for all $n\geq 1$.

30. Suppose $a_1=3$ and $a_n=2a_{n-1}-n+2$ for $n\geq 2$. Prove that $a_n=2^n+n$ for all positive integers n.
Basis step: The formula is true for $n=1$,
$$a_1=3=2^1+1$$
Inductive step: Let $k\geq 1$ be a natural number. Suppose that the formula is true for $0\leq n\leq k$, i.e., $a_k=2^k+k$. Then
$$a_{k+1}=2a_k-(k+1)+2=2\left(2^k+k\right)-k+1=2^{k+1}+(k+1)$$
So the formula is true for $n=k+1$, and by induction, it is true for all $n\geq 1$.

31. Suppose $b_1=3$, $b_2=9$, and for $n\geq 3$, $b_n=2b_{n-1}+3b_{n-2}$. Prove that $b_n=3^n$ for all positive integers n.
Basis step: Since we have two basis definitions, for $n=1$ and $n=2$, we need to verify that
$$b_1=3=3^1$$
$$b_2=9=3^2$$
Inductive step: We use strong induction. Let $k\geq 2$ be a natural number, we assume that the formula is true for $0\leq n\leq k$. Then
$$b_{k+1}=2b_k+3b_{k-1}=2\left(3^k\right)+3\left(3^{k-1}\right)=3^{k-1}(2\cdot 3+3)=9\cdot 3^{k-1}=3^{k+1}$$
Therefore the formula is true for $n=k+1$, and by induction, the formula is true for all $n\geq 1$.

32. Prove that $\binom{3}{3}+\binom{4}{3}+\cdots+\binom{n-1}{3}+\binom{n}{3}=\binom{n+1}{4}$ for every positive integer $n\geq 3$.
Basis step: The formula is true for $n=3$, $\binom{3}{3}=1=\binom{4}{4}$.
Inductive step: Let $k\geq 3$ be a natural number. Suppose that the formula is true for $n=k$, that is,
$$\binom{3}{3}+\binom{4}{3}+\cdots+\binom{k-1}{3}+\binom{k}{3}=\binom{k+1}{4}$$
Then
$$\binom{3}{3}+\binom{4}{3}+\cdots+\binom{k-1}{3}+\binom{k}{3}+\binom{k+1}{3}=\binom{k+1}{4}+\binom{k+1}{3}=\binom{k+1}{4}$$
where the last identity comes from the Pascal identity: $\binom{n}{k}=\binom{n-1}{k-1}+\binom{n-1}{k}$
So the formula is true for $n=k+1$, and by induction, it is true for all $n\geq 3$.