# *CSE 1400 Applied Discrete Mathematics*
# *Number Theory and Proofs*

*Department of Computer Sciences*

*College of Engineering*

*Florida Tech*

*Spring 2012*

Problems labeled

⚠ are important and must be mastered.

are harder and cover interesting advanced material that is not properly part of this course.

are tangential to the course but cover material that is useful elsewhere.

## *Problems for Number Theory*

**Background**

Number theory is the branch of mathematics that studies properties of the integers. Prime numbers are a major topic in number theory. There are many practical applications of number theory, for instance, cryptology, random number generation, and check digits in codes.

1. ⚠ Answer the following `True` or `False`.

   (a) The set of prime numbers is

   $$\mathbb{P} = \{2, 3, 5, 7, 11, 13, \ldots\} = \{p \in \mathbb{N} : p \text{ has exactly two different divisors.}\}$$

   Answer: This is `True`.

   (b) The integer 1 is prime because it is divisible by itself and 1.
   Answer: This is `False`.

   (c) The set of composite numbers is

   $$\mathbb{C} = \{4, 6, 8, 9, 10, 11, \ldots\} = \{c \in \mathbb{N} : c \text{ more than two different divisors.}\}$$

   Answer: This is `True`.

   (d) Every natural number can be written as the products of prime numbers, that is
   Answer: This is `False`. Both 0 and 1 are counterexamples. They are natural numbers that cannot be written as the product of primes.

   (e) Every natural number greater than 1 can be written as the products of prime numbers.
   Answer: This is `True`. It is known as the Fundamental Theorem of Arithmetic.

   (f) There are infinitely many primes, that is,

   $$(\forall p \in \mathbb{P})(\exists q \in \mathbb{P})(q > p)$$

   Answer: This is `True`.

   (g) There is a largest prime number, that is

   $$(\exists p \in \mathbb{P})(\forall q \in \mathbb{P})(q \leq p)$$

   Answer: This is `False`. The proposition states there is a largest prime number $p$, which is not `True`.

2. A repeated product can be written using PRODUCT notation

$$\prod_{k=0}^{n-1} a_k = a_0 a_1 \cdots a_{n-1}$$

(a) Write $n$ factorial ($n!$) using product notation
Answer:

$$n! = n(n-1)(n-2)\cdots 2 \cdot 1 = \prod_{k=0}^{n-1}(k+1)$$

(b) Write the binomial coefficient $\binom{n}{m}$ using product notation
Answer: Pretend that $n - m \geq m$.

$$\begin{aligned}\binom{n}{m} &= \frac{n!}{m!(n-m)!} \\ &= \frac{\prod_{k=0}^{n-1}(k+1)}{\prod_{k=0}^{m-1}(k+1)\prod_{k=0}^{n-m-1}(k+1)} \\ &= \frac{\prod_{k=0}^{n-m}(k+1)}{\prod_{k=n-m+1}^{n-1}(k+1)}\end{aligned}$$

(c) The natural value to assign to the empty product $\prod_{k=0}^{-1} k$ is 1.
Answer: This is `True`.

## *Problems on Modular Numbers*

**Background**

The integers mod $n$ are

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, (n-1)\}$$

where each $k$ value represent the set of values

$$\{an + k : a \in \mathbb{Z}\}$$

1. Describe the residue (equivalence) classes for

(a) Congruence mod 4.
Answer:

$$\begin{aligned}[0] &= \{4k : k \in \mathbb{Z}\} \\ [1] &= \{4k+1 : k \in \mathbb{Z}\} \\ [2] &= \{4k+2 : k \in \mathbb{Z}\} \\ [3] &= \{4k+3 : k \in \mathbb{Z}\}\end{aligned}$$

(b) Congruence mod 5.
Answer:

$$
\begin{aligned}
[0] &= \{5k : k \in \mathbb{Z}\} \\
[1] &= \{5k+1 : k \in \mathbb{Z}\} \\
[2] &= \{5k+2 : k \in \mathbb{Z}\} \\
[3] &= \{5k+3 : k \in \mathbb{Z}\} \\
[4] &= \{5k+4 : k \in \mathbb{Z}\}
\end{aligned}
$$

2. How many residue classes are there mod $n$?
Answer: There are $n$ residue classes, named $[0]$ through $[n-1]$.

3. For the given values of $a$ and $n$ below, compute the quotient $q$ and non-negative remainder $r$ that satisfy the quotient-remainder equation

$$a = qn + r, \quad r \geq 0$$

(a) $a = 26$, $n = 13$.
(b) $a = 27$, $n = 13$.
(c) $a = -27$, $n = 13$.
(d) $a = -45$, $n = 13$.

4. Construct an addition table for the integers mod 6.
Answer:

| + | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

5. Construct a multiplication table for the integers mod 4.
Answer:

| × | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

6. Construct a multiplication table for the integers mod 7.

Answer:

| $\times$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 0 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 0 | 6 | 5 | 4 | 3 | 2 | 1 |

7. Solve the following linear congruence equations.
   (a) $3x \equiv 5 \pmod 7$
   Answer: $x = 4$ since $3 \cdot 4 = 12 = 5 \pmod 7$.
   (b) $5x \equiv 4 \pmod 7$
   Answer: $x = 5$ since $5 \cdot 5 = 25 = 4 \pmod 7$.
   (c) $2x \equiv 1 \pmod 7$
   Answer: $x = 4$ since $2 \cdot 1 = 8 = 1 \pmod 7$.
   (d) $6x \equiv 3 \pmod 7$
   Answer: $x = 4$ since $6 \cdot 4 = 24 = 3 \pmod 7$.
8. Given the values of $p$ and $q$ below: What is their greatest common divisor $\gcd(p, q)$? What is their least common multiple of $\operatorname{lcm}(p, q)$? Verify the $\gcd(p, q) \cdot \operatorname{lcm}(p, q) = pq$.
   (a) Let $p = 2^5 3^4 11^7 13^{10} 19^6$ and $q = 3^6 11^5 13^{12} 17^4$.
9. Use Euclid's algorithm to compute the greatest common divisors listed below.
   (a) $\gcd(19, 8)$.
   Answer:

$$\begin{aligned} 19 &= 8 \cdot 2 + 3 \\ 8 &= 3 \cdot 2 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

   The greatest common denominator is 1.
   (b) $\gcd(25, 40)$.
   Answer:

$$\begin{aligned} 25 &= 40 \cdot 0 + 25 \\ 40 &= 25 \cdot 1 + 15 \\ 25 &= 15 \cdot 1 + 10 \\ 15 &= 10 \cdot 1 + 5 \\ 10 &= 5 \cdot 2 + 0 \end{aligned}$$

The greatest common denominator is 5.

(c) $\gcd(70, 27)$.
Answer:

$$\begin{aligned} 70 &= 27 \cdot 2 + 16 \\ 27 &= 16 \cdot 1 + 11 \\ 16 &= 11 \cdot 1 + 5 \\ 11 &= 5 \cdot 2 + 1 \\ 5 &= 1 \cdot 5 + 0 \end{aligned}$$

$\therefore \gcd(27, 70) = 1$.

(d) $\gcd(66, 99)$.
Answer:

$$\begin{aligned} 99 &= 66 \cdot 1 + 33 \\ 66 &= 33 \cdot 2 + 0 \end{aligned}$$

$\therefore \gcd(66, 99) = 33$.

(e) $\gcd(189, 80)$.

(f) $\gcd(511, 255)$.
Answer:

$$\begin{aligned} 511 &= 255 \cdot 2 + 1 \\ 255 &= 1 \cdot 255 + 0 \end{aligned}$$

$\therefore \gcd(511, 255) = 1$.

10. Using your work from question 9 find integers $a$ and $b$ such that

(a) $1 = 19a + 8b$.
Answer: Fill in the "magic table" using the quotients from the Euclidean algorithm. Start from the initial two columns and compute next columns by the recurrence

$$c_n = qc_{n-1} + c_{n-2}$$

| 19 | 8 | 2 | 2 | 1 | 2 |
|---|---|---|---|---|---|
| 0 | 1 | 2 | 5 | 7 | 19 |
| 1 | 0 | 1 | 2 | 3 | 8 |

$\therefore 1 = 19 \cdot (-3) + 8 \cdot 7$ where $a = -3$ and $b = 7$.

(b) $5 = 40a + 25b$.
Answer: Fill in the "magic table" using the quotients from the Euclidean. Start from the initial two columns and compute next columns by the recurrence

$$c_n = qc_{n-1} + c_{n-2}$$

| 40 | 25 | 1 | 1 | 1 | 2 |
|---|---|---|---|---|---|
| 0 | 1 | 1 | 2 | 3 | 8 |
| 1 | 0 | 1 | 1 | 2 | 5 |

$\therefore 1 = 5 \cdot 3 + 8 \cdot (-2)$ and, multiplying this equation through by 5 gives $5 = 5 \cdot 15 + 8 \cdot (-10)$

(c) $1 = 70a + 27b$.
Answer: Fill in the "magic table" using the quotients from the Euclidean Start from the initial two columns and compute next columns by the recurrence

$$c_n = qc_{n-1} + c_{n-2}$$

| 70 | 27 | 2 | 1 | 1 | 2 | 5 |
|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 5 | 13 | 70 |
| 1 | 0 | 1 | 1 | 2 | 5 | 27 |

$\therefore 1 = 70 \cdot (-5) + 27 \cdot (13)$.

(d) $33 = 66a + 99b$.
Answer: Fill in the "magic table."

| 99 | 66 | 1 | 2 |
|---|---|---|---|
| 0 | 1 | 1 | 3 |
| 1 | 0 | 1 | 2 |

$\therefore -1 = 2 \cdot 1 + 3 \cdot (-1)$ and, multiplying this equation by $-33$ we get $33 = 66 \cdot (-1) + 99 \cdot 1$.

11. Using your work from question 10, solve the following linear congruence equations.

(a) $8x = 5 \bmod 19$.
Answer: Since $19 \cdot (-3) + 8 \cdot 7 = 1$, $8 \cdot 7 = 1 \bmod 19$ it follows that $x = 7 \cdot 8x = x = 7 \cdot 5 = 35 = 16 \bmod 19$.

(b) $25x = 38 \bmod 40$.
Answer:

(c) $27x = 4 \bmod 70$.
Answer: Since $70 \cdot (-5) + 27 \cdot 13 = 1$, $27 \cdot 13 = 1 \bmod 70$ it follows that $x = 13 \cdot 27x = x = 13 \cdot 4 = 52 \bmod 70$.

(d) $66x = 22 \mod 99$.
Answer:

## *Problems on Proofs*

**Background**

Statements have been proved throughout the course. Now these ideas will be organized into proof methods.

### *Vacuous and Trivial Proofs*

**Background**

A statement of the form

$$\texttt{False} \to \mathrm{P}$$

is vacuously `True`.

A statement of the form

$$\mathrm{P} \to \texttt{True}$$

is trivially `True`.

1. Prove that the empty set is a subset of every set.

   Answer: $\mathbb{X}$ is a subset of $\mathbb{Y}$ if for every $x \in \mathbb{X}$, $x \in \mathbb{Y}$. The statement

   $$(\forall x \in \mathbb{U})(x \in \emptyset \to x\mathbb{Y})$$

   is vacuously `True` because $x \in \emptyset$ is `False`.

2. Prove that less than is antisymmetric.

   Answer: There is a vacuous proof: The statement that less than is antisymmetric is $(\forall x, y \in \mathbb{R})((x < y \wedge y < x) \to (x = y))$, which is `True` by virtue of its logical form: $\mathrm{P} \to \mathrm{Q}$ where the premise $\mathrm{P} = (x < y \wedge y < x)$ is always `False` which makes the conditional always `True`.

## *Direct Proofs*

**Background**

Direct proofs may be the most common. They rely on the modus ponens rule of inference

$$(\mathrm{P} \wedge (\mathrm{P} \to \mathrm{Q}) \to \mathrm{Q}$$

That is, if $\mathrm{P}$ is `True` and $\mathrm{P} \to \mathrm{Q}$ is `True`, then $\mathrm{Q}$ must be `True`.

1. Let $x = a \bmod n$ and $y = b \bmod n$. Prove that $x + y = (a + b) \bmod n$.

   Answer: If $x = a \bmod n$ and $y = b \bmod n$, then $x - a = nc$ and $y - b = nd$ for some integers $c$ and $d$. Therefore $(x - a) + (y - b) = (x + y) - (a + b) = nc + nd = n(c + d)$, that is $x + y = (a + b) \bmod n$.

2. Let $x = a \bmod n$ and $y = b \bmod n$. Prove that $xy = ab \bmod n$.

   Answer: If $x = a \bmod n$ and $y = b \bmod n$, then $x - a = nc$ and $y - b = nd$ for some integers $c$ and $d$. Therefore $(x - a)(y - b) = xy - ay - bx + ab =$, that is $x + y = (a + b) \bmod n$.

3. Prove that if the integers $m$ and $n$ are both odd, then $mn$ is odd.

   Answer: If $m$ and $n$ are odd, then $m = 2k + 1$ and $n = 2j + 1$ for some integers $k$ and $j$. Therefore

   $$\begin{aligned} mn &= (2k+1)(2j+1) \\ &= 4kj + 2k + 2j + 1 \\ &= 2(kj + k + j) + 1 \end{aligned}$$

   which shows $mn$ is odd.

4. Prove that $(1 + \sqrt{5})/2$ and $(1 - \sqrt{5})/2$ are solutions to the equation $x^2 = x + 1$.

   Answer: The quadratic formula computes the two solutions to the quadratic equation $x^2 - x - 1 = 0$ as $(1 + \sqrt{5})/2$ and $(1 - \sqrt{5})/2$.

5. Prove that if $n$ is even then $n^2$ is even and if $n$ is odd then $n^2$ is odd.
   Answer: If $n = 2k$ is even, then $n^2 = 4k^2$ is even. If $n = 2k+1$ is odd, then $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ is odd.
6. Prove that if $n$ is an even integer, then $n = 4k$ or $n = 4k+2$ for some integer $k$.
   Answer: If $n$ is even, then $n = 2m$ for some integer $m$. If $m$ is even, that is, if $m = 2k$, then $n = 2m = 2(2k) = 4k$. If $m$ is odd, that is, if $m = 2k+1$, then $n = 2m = 2(2k+1) = 4k+2$.
7. Prove that $(\forall x \in \mathbb{R},\, x \geq 0)(\sqrt{x(x+2)} < x+1)$.
   Answer: Square the left-hand side of the inequality to obtain

$$\begin{aligned}(\sqrt{x(x+2)})^2 &= x(x+2)\\ &= x^2 + 2x\\ &< x^2 + 2x + 1\\ &= (x+1)^2\end{aligned}$$

   which shows the result is `True`.
8. (Quotient–Remainder Lemma 1) Given integers $a$, $n \in \mathbb{Z}$, $n \neq 0$, consider the set of natural numbers

$$\mathbb{A} = \{a - nq \geq 0 : q \in \mathbb{Z}\}$$

   Prove $\mathbb{A}$ is not empty.
   Answer: To see this, let

$$q = \begin{cases} \lfloor a/n \rfloor & \text{if } n > 0, \text{ that is, } a \geq nq \text{ if } a/n \geq q. \\ \lceil a/n \rceil & \text{if } n < 0, \text{ that is, } a \geq nq \text{ if } a/n \leq q. \end{cases}$$

   Since $\lfloor a/n \rfloor \leq a/n \leq \lceil a/b \rceil$, the first case, when $n > 0$, $q = \lfloor a/n \rfloor \leq a/n$ implies $a - nq \geq 0$. And, in the second case, when $n < 0$, $a/n \leq \lceil a/n \rceil = q$, implies $a - qn \geq 0$. In both cases, there is an element in $\mathbb{A}$
9. Prove that $\lg n! \leq n \lg n$.
   Answer: By the "log of a product is the sum of logs" rule

$$\lg(n!) = \lg n(n-1)(n-2)\cdots 2 \cdot 1 = \lg(n) + \lg(n-1) + \lg(n-2) + \cdots + \lg(2) + \lg(1)$$

   For each $k = 1, 2, \ldots, n$, $\lg(k) \leq \lg(n)$ Therefore

$$\lg(n!) = \lg(n) + \lg(n-1) + \lg(n-2) + \cdots + \lg(2) + \lg(1) \leq n \lg(n)$$

10. (Euclid's Lemma) Let $p \in \mathbb{P}$ be a prime number and let $a$, $b \in \mathbb{N}$ be natural numbers. If $p$ divides $ab$, then $p$ divides $a$ or $p$ divides $b$.
    Answer: Pretend $p$ divides $ab$ and $p$ does not divide $a$. That is,

$$(\exists c \in \mathbb{N})(pc = ab) \wedge (a \bmod p = r \neq 0)$$

    By the fundamental theorem of arithmetic, $ab$ can be factored as a product of primes. Since $p$ does not divide $a$, $p$ is not one of the prime factors of $a$. Therefore, since the prime factorization is unique, $p$ must be a prime factor of $b$. That is, $p$ divides $b$.

## *Proof by Contraposition*

**Background**

Proofs by contraposition are indirect proofs. To prove

$$P \to Q$$

prove

$$\neg Q \to \neg P$$

instead.

1. Prove that if $n^2$ is even then $n$ is even.
   Answer: If $n$ is odd, then $n = 2k + 1$ and $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ is odd.
2. Prove that if $n^2$ is odd then $n$ is odd.
   Answer: If $n$ is even, then $n = 2k$ and $n^2 = 4k^2 = 2(2k^2)$ is even.

## *Proofs by Contradiction*

**Background**

Suppose that

$$\neg P \to Q$$

and

$$\neg P \to \neg Q$$

are both `True`. Then it must be that $\neg P$ is `False`, that is, $P$ is `True`. The conjunction

$$Q \wedge \neg Q$$

is a contradiction and showing

$$\neg P \to Q \wedge \neg Q$$

is `True` proves that $P$ is `True`.

1. If $n^2 - 1$ is not divisible by 8, then $n$ is even.
   Answer: Note that the form of the statement is

   $$P \to Q \equiv \neg P \vee Q$$

   which has negation

   $$P \wedge \neg Q$$

   Assume $n^2 - 1$ is not divisible by 8 and $n$ is odd. Then $n = 2k + 1$ for some integer $k$ and $n^2 - 1 = 4k^2 + 4k = 4k(k + 1)$. Since $k$ and $k + 1$ are consecutive integers one of them is even, so in fact, $4k(k + 1)$ is divisible by 8.
2. Prove that $\sqrt[3]{2}$ is irrational.
   Answer: By way of contradiction, pretend $\sqrt[3]{2}$ is rational and let $\sqrt[3]{2} = a/b$ where $a$ and $b$ are relatively prime integers with $b \neq 0$. Then

   $$\begin{aligned} \sqrt[3]{2} &= \frac{a}{b} \\ 2 &= \frac{a^3}{b^3} \\ 2b^3 &= a^3 \end{aligned}$$

and so $a$ is a multiple of 2. Let $a = 2k$, then

$$\begin{aligned} 2b^3 &= 8a^3 \\ b^2 &= 4a^3 \end{aligned}$$

and so $b$ is a multiple of 2. This contradicts that $a$ and $b$ are relatively prime.

3. Prove that if $k < \sqrt{n} < k+1$ for some integer $k$, then $\sqrt{n}$ is irrational.
   Answer: Assume $\sqrt{n}$ is rational.

$$\begin{aligned} \sqrt{n} &= \frac{a}{b}, \quad a, b \in \mathbb{Z}, b \neq 0, \gcd(a, b) = 1 \\ \sqrt{n}b &= a \\ nb^2 &= a^2 \end{aligned}$$

$n$ divides $a^2$. Let

$$n = \prod_{k=0}^{m-1} p_k^{e_k}$$

be the prime factorization of $n$, and let

$$a = \prod_{k=0}^{j-1} q_k^{f_k}$$

be the prime factorization of $a$. Since $n \mid a^2$ each prime factor $p_k^{e_k}$ of $n$ must divide one of the prime factors of $a$. Therefore $n$ divides $a$ and $a = nc$ for some natural number $c$. But then $nb^2 = a^2 = n^2c^2$ and $b^2 = nc^2$. That is $n$ divides both $a$ and $b$ which contradicts that $a$ and $b$ are relatively prime.

## *Proofs by Counterexample*

**Background**

A universally quantified statement such as

$$(\forall x \in \mathbb{U})(\mathrm{P}(x))$$

can be proved `False` by giving one instance (a counterexample) where it is `False`.

1. (Be able to construct counterexamples) Give a counterexample to prove that the following universally quantified statements are false
   (a) If $n$ an even natural number then $n + m$ is even for all natural numbers $m$.
   Answer: Let $n = 0$ and $m = 1$. Then $n$ is even and $n + m = 1$ is odd.
   (b) If natural number $n > 0$ is a multiple of 3, then $n^2 - 1$ is divisible by 4.
   Answer: The statement is `True` for $n = 1$ and $n = 3$: Both 0 and 8 are divisible by 4, but for $n = 6$, $n^2 - 1 = 35$ is not divisible by 4.
   (c) If $a$ and $b$ are rational numbers, then $a^b$ is a rational number.
   Answer: Let $a = 2$ and $b = 1/2$. Then $a^b = 2^{1/2} = \sqrt{2}$ is an irrational number.
   (d) If $a^2$ is a multiple of $b$, then $a$ is a multiple of $b$.
   Answer: Let $a = 2$ and $b = 4$. Then $a^2 = 4$ is a multiple of $b = 4$, but $a = 2$ is not a multiple of $b = 4$.

## *Mathematical Induction*

**Background**

Mathematical induction is one of the most important proof techniques in discrete mathematics. To prove that $\mathrm{P}(n)$ is `True` for all natural numbers $n$ it suffices to show

$$\mathrm{P}(0) \wedge (\mathrm{P}(n) \rightarrow \mathrm{P}(n+1)) \quad \text{is } \texttt{True}$$

1. Prove that the sum of the first $n$ natural numbers is $n(n-1)/2$.

   Answer: The natural numbers lie in the set

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, 6, \ldots\}$$

   The sum of the first $n$ natural numbers is

$$0 + 1 + 2 + 3 + \cdots + (n-1)$$

   Basis for Induction: For $n = 0$ the sum on the left-hand side of the equality is empty and has value zero. Also, the right-hand side expression is $0(0-1)/2$ is also zero.

   Inductive Premise: Pretend the equality

$$\sum_{k=0}^{n-1} k = \frac{n(n-1)}{2}$$

   is `True` for some $n \geq 0$.

   Inductive Step: If

$$\sum_{k=0}^{n-1} k = \frac{n(n-1)}{2}$$

   then

$$\begin{aligned}\sum_{k=0}^{n} k &= \sum_{k=0}^{n-1} k + n \\ &= \frac{n(n-1)}{2} + n \\ &= \frac{n(n-1)}{2} + \frac{2n}{2} \\ &= \frac{n(n-1) + 2n}{2} \\ &= \frac{n(n+1)}{2}\end{aligned}$$

   establishing that if the equality holds for $n$, then it holds for $n+1$.

   Conclusion:

$$\sum_{k=0}^{n} k = \frac{n(n-1)}{2} \quad (\forall n \in \mathbb{N})$$

2. Prove the formula for arithmetic sums

$$(\forall n \in \mathbb{N})(\forall m, b \in \mathbb{R})(b + (m+b) + (2m+b) + \cdot + (nm+b) = (n+1)\frac{nm+2b}{2}$$

That is, the sum of terms in the arithmetic sequence

$$\vec{\mathcal{A}} = \langle b,\, m+b,\, b+2m, \ldots,\, b+nm \rangle$$

is the number of terms time the average of the first and last term.

Answer: For $n = 0$, the sum on the left of the equality is equal to $b$ and the function on n the right of the equality is equal to $(0+1)\frac{0m+2b}{2} = b$. Assume that

$$(\exists n \in \mathbb{N})(\forall m,\, b \in \mathbb{R})(b + (m+b) + (2m+b) + \cdots + (nm+b) = (n+1)\frac{nm+2b}{2}$$

Then

$$\begin{aligned}
b + (m+b) + (2m+b) + \cdots + (nm+b) + ((n+1)m+b) &= (n+1)\frac{nm+2b}{2} + ((n+1)m+b) \\
&= \frac{n(n+1)m + 2(n+1)b}{2} + \frac{2(n+1)m+2b)}{2} \\
&= \frac{n(n+1)m + 2(n+1)b + 2(n+1)m + 2b}{2} \\
&= \frac{(n+2)(n+1)m + 2(n+2)b}{2} \\
&= (n+2)\frac{(n+1)m+2b}{2}
\end{aligned}$$

3. Prove that the sum of the first $n$ powers of 2 is $2^n - 1$.

Answer:

Basis for Induction: For $n = 0$ the sum on the left-hand side of the equality is empty and has value zero. Also, the right-hand side expression $2^0 - 1$ is zero also.

Inductive Premise: Pretend the equality

$$\sum_{k=0}^{n-1} 2^k = 2^n - 1$$

is `True` for some $n \geq 0$.

Inductive Step: If

$$\sum_{k=0}^{n-1} 2^k = 2^n - 1$$

then

$$\begin{aligned}
\sum_{k=0}^{n} 2^k &= \sum_{k=0}^{n-1} 2^k + 2^n \\
&= (2^n - 1) + 2^n \\
&= 2 \cdot 2^n - 1 \\
&= 2^{n+1} - 1
\end{aligned}$$

establishing that if the equality holds for $n$, then it holds for $n+1$.

Conclusion:

$$\sum_{k=0}^{n} 2^k = 2^n - 1 \quad (\forall n \in \mathbb{N})$$

4. Prove the formula for geometric sums

$$(\forall n \in \mathbb{N})(\forall r \in \mathbb{R}, r \neq 1)(a + ar + ar^2 + \cdots + ar^{n-1} = a\frac{r^n - 1}{r - 1}$$

Answer: For $n = 0$, the sum on the left of the equality is empty and equal to 0 and the function on the right of the equality is also equal to 0. Assume that

$$(\exists n \in \mathbb{N})(\forall r \in \mathbb{R}, r \neq 1)(a + ar + ar^2 + \cdots + ar^{n-1} = a\frac{r^n - 1}{r - 1}$$

Then

$$\begin{aligned} a + ar + ar^2 + \cdots + ar^{n-1} + ar^n &= a\frac{r^n - 1}{r - 1} + ar^n \\ &= a\frac{r^n - 1}{r - 1} + \frac{ar^n(r-1)}{r - 1} \\ &= a\frac{r^n - 1 + r^{n+1} - r^n}{r - 1} \\ &= a\frac{r^{n+1} - 1}{r - 1} \end{aligned}$$

5. Prove the fundamental theorem of arithmetic: Every natural number $n > 1$ can be written as the product of primes. (Note that a product may be a single factor so that a prime $p$ is itself a product of primes.)

Answer:

Basis: Let $n = 2$. Since 2 is prime, it is a product of primes.

Inductive Hypothesis: Let $n \geq 3$ and suppose every natural number from 2 to $n - 1$ can be written as the product of primes.

Inductive Step: Consider the natural number $n$. If $n$ is prime, then it is the product of primes. If $n$ is composite, then $n = a \cdot b$ for some natural numbers $a$, $b < n$. By the inductive hypothesis, both $a$ and $b$ can be written as the product of primes. Therefore, $n$ can be written as the product of primes.

6. Prove that $(\forall n \in \mathbb{N}, n > 0)(3^n > 2^n)$.

Answer: For $n = 1$, $3 > 2$ establishing a basis for induction. Assume that $(\exists n \in \mathbb{N}, n > 0)(3^n > 2^n)$. Then $3^{n+1} = 3 \cdot 3^n > 3 \cdot 2^n > 2 \cdot 2^n = 2^{n+1}$.

7. Prove that for all natural numbers and all real numbers $a$ and $b$

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots ab^{n-2} + b^{n-1})$$

Answer: Notice that

$$a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots ab^{n-2} + b^{n-1} = \sum_{k=0}^{n-1} a^{n-1-k}b^k$$

In particular, the sum is empty and equal to 0 when $n = 0$. Therefore, for $n = 0$ the left-hand side of the equality is $a^0 - b^0 = 0$ and the right-hand side is $(a - b)$ time the empty sum and equal to 0 also. We can also assume that $a \neq b$ since both sides of the equation are equal to 0 when $a = b$. Now assume that

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots ab^{n-2} + b^{n-1})$$

for some $n \geq 0$. Then

$$\begin{aligned}
\sum_{k=0}^{n} a^{n-k}b^k &= \sum_{k=0}^{n-1} a^{n-k}b^k + b^n \\
&= a\sum_{k=0}^{n-1} a^{n-1-k}b^k + b^n \\
&= a\frac{a^n - b^n}{a - b} + b^n \\
&= a\frac{a^n - b^n}{a - b} + b^n\frac{a - b}{a - b} \\
&= \frac{a^{n+1} - ab^n + b^n a - b^{n+1}}{a - b} \\
&= \frac{a^{n+1} - b^{n+1}}{a - b}
\end{aligned}$$

The sum

$$\sum_{k=0}^{n} a^{n-k}b^k = a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots ab^{n-2} + b^{n-1}$$

is called the "convolution" of finite sequences

$$\left\langle a^{n-1}, a^{n-2}, a^{n-3}, \cdots, a, 1 \right\rangle \quad \text{and} \left\langle 1, b, b^2, b^3, \cdots, b^{n-1} \right\rangle$$

8. Let $a = (1 + \sqrt{5})/2$ denote the golden ratio and let $b = (1 - \sqrt{5})/2$ be its conjugate. Show that

$$F_n = \frac{a^n - b^n}{a - b}$$

where $F_n$ is the Fibonacci number.

Answer: Since seeding the Fibonacci recurrence requires 2 values, we need to establish the basis for both $n = 0$ and $n = 1$. First, $F_0 = 0$ and $\frac{a^0 - b^0}{a - b} = 0$ also. Second, $F_1 = 1$ and $\frac{a^1 - b^1}{a - b} = 1$ also. Now assume that

$$F_n = \frac{a^n - b^n}{a - b} \quad \text{and} \quad F_{n-1} = \frac{a^{n-1} - b^{n-1}}{a - b}$$

for some pair $n$ and $n - 1$ where $n \geq 1$. Recall, from problem 4 that $(1 + \sqrt{5})/2$ and $(1 - \sqrt{5})/2$ are

solutions to the equation $x^2 = x + 1$. Then

$$\begin{aligned}
F_{n+1} &= F_n + F_{n-1} \\
&= \frac{a^n - b^n}{a - b} + \frac{a^{n-1} - b^{n-1}}{a - b} \\
&= \frac{a^n - b^n}{a - b} + \frac{a^{n-1} - b^{n-1}}{a - b} \\
&= \frac{a^n - b^n + a^{n-1} - b^{n-1}}{a - b} \\
&= \frac{a^{n-1}(a+1) - b^{n-1}(b+1)}{a - b} \\
&= \frac{a^{n-1}a^2 - b^{n-1}b^2}{a - b} \\
&= \frac{a^{n+1} - b^{n+1}}{a - b}
\end{aligned}$$

9. Let $n > 0$ and prove that the Fibonacci numbers $F_n$ and $F_{n+1}$ are relatively prime.
   Answer:

10. Prove that
$$(\forall n \in \mathbb{N},\, n > 1)(\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{(n-1) \cdot n} = \frac{n-1}{n})$$

   Answer: For $n = 2$, $1/(1 \cdot 2) = (2-1)/2$ establishing a basis for induction. Assume that
$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{(n-1) \cdot n} = \frac{n-1}{n}$$
   for some $n \geq 2$. Then
$$\begin{aligned}
\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{(n-1) \cdot n} + \frac{1}{n \cdot (n+1)} &= \frac{n-1}{n} + \frac{1}{n(n+1)} \\
&= \frac{(n-1)(n+1)}{n(n+1)} + \frac{1}{n(n+1)} \\
&= \frac{n^2}{n(n+1)} \\
&= \frac{n}{n+1}
\end{aligned}$$

11. Using the result in problem 10, give a direct proof that
$$(\forall n \in \mathbb{N},\, n > 1)(\frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots + \frac{1}{n^2} < 1)$$
   (Interestingly, as $n$ tends toward infinity, the sum converges to $\pi^2/6$.)

Answer: For any $n > 1$, $n > n - 1$ which implies $1/(n-1) > 1/n$. Therefore

$$\frac{1}{n(n-1)} > \frac{1}{n^2} \text{ for all } n > 1$$

Sum both sides of this inequality from $k = 2$ to $k = n$ to obtain

$$\begin{aligned}\frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} &< \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{(n-1) \cdot n} \\ &= \frac{n-1}{n} \\ &< 1\end{aligned}$$

12. Prove that for any $n > 0$

$$1^2 + 4^2 + 7^2 + 10^2 + \cdots + (3n-2)^2 = \frac{n(6n^2 - 3n - 1)}{2}$$

Answer: For $n = 1$, $1^2 = 1 = 1(6 - 3 - 1)/2$ establishing a basis for induction. Assume that

$$1^2 + 4^2 + 7^2 + 10^2 + \cdots + (3n-2)^2 = \frac{n(6n^2 - 3n - 1)}{2}$$

for some $n > 0$. Then

$$\begin{aligned}1^2 + 4^2 + 7^2 + 10^2 + \cdots + (3n-2)^2 + (3n+1)^2 &= \frac{n(6n^2 - 3n - 1)}{2} + (3n+1)^2 \\ &= \frac{6n^3 - 3n^2 - n}{2} + (9n^2 + 6n + 1) \\ &= \frac{6n^3 - 3n^2 - n}{2} + \frac{18n^2 + 12n + 2}{2} \\ &= \frac{6n^3 + 15n^2 + 11n + 2}{2} \\ &= \frac{6(n^3 + 3n^2 + 3n + 1) - 3(n^2 + 2n + 1) - (n+1)}{2} \\ &= \frac{6(n+1)^3 - 3(n+1)^2 - (n+1)}{2} \\ &= \frac{(n+1)(6(n+1)^2 - 3(n+1) - 1)}{2}\end{aligned}$$

13. Prove that for all $n \geq 2$

$$\sqrt{2\sqrt{3\sqrt{4 \cdots \sqrt{n-1}\sqrt{n}}}} < 3$$

Answer: For $n = 2$, $\sqrt{2} \approx 1.414 < 3$ establishing a basis for induction. Assume $\sqrt{2\sqrt{3\sqrt{4 \cdots \sqrt{n-1}\sqrt{n}}}} < 3$ for some $n \geq 2$. Then $\sqrt{2\sqrt{3\sqrt{4 \cdots \sqrt{n-1}\sqrt{n}}}} < 3$

14. Prove that for any $n \in \mathbb{N}$, $2^{3^n} = 2 \pmod 3$.
Answer: For $n = 0$, $2^{3^0} = 2 = 2 \pmod 3$. Assume $2^{3^n} = 2 \pmod 3$ for some $n \geq 0$. Then

$$\begin{aligned} 2^{3^{n+1}} &= 2^{3 \cdot 3^n} \\ &= 2^{3^n} 2^{3^n} 2^{3^n} \\ &= (2^{3^n})^3 \\ &= 2^3 \pmod 3 \\ &= 8 \pmod 3 \\ &= 2 \pmod 3 \end{aligned}$$

15. Prove that $3^{n+1}$ divides $2^{3^n} + 1$ for all natural numbers.
Answer: For $n0$, $3^{n+1} = 3$ which divides $2^{3^n} + 1 = 2^{3^0} + 1 = 3$ establishing a basis for induction. Assume $3^{n+1}$ divides $2^{3^n} + 1$ for some $n \geq 0$. We need to show that $3^{n+2}$ divides $2^{3^{n+1}} + 1$. By our assumption $3^{n+1}$ divides $2^{3^n} + 1$ so to complete the proof we only need to show 3 divides $(2^{3^n})^2 - \cdot 2^{3^n} + 1$. By problem 14 $2^{3^n} = 2 \pmod 3$ and so its square is $\left(2^{3^n}\right)^2 = 2^2 \pmod 3 = 4 \pmod 3 = 1 \pmod 3$. Therefore $(2^{3^n})^2 - \cdot 2^{3^n} + 1 = 1 - 2 + 1 \pmod 3 = 0 \pmod 3$.

16. Prove that $r - 1$ divides $r^n - 1$ for all natural numbers $r \neq 1$ and $n$.
Answer: Let $r \neq 1$ be fixed but otherwise arbitrary. Using induction on $n$: For $n = 0$, $r - 1$ divides $r^0 - 1 = 0$. If $r - 1$ divides $r^n - 1$, that is, if $(r-1)c = r^n - 1$ for some natural number $c$, then

$$\begin{aligned} r^{n+1} - 1 &= r^{n+1} - r^n + r^n - 1 \\ &= r^n(r-1) + (r^n - 1) \\ &= r^n(r-1) + (r-1)c \\ &= (r-1)(r^n + c) \end{aligned}$$

Showing that $r - 1$ divides $r^{n+1} - 1$. Recall the geometric sum formula

$$\sum_{k=0}^{n-1} r^k = \frac{r^n - 1}{r - 1} \quad \text{for } r \neq 1$$

17. Prove that

$$\sum_{k=0}^{n} \binom{n}{n+k} \frac{1}{2^k} = 2^n$$

Answer: For $n = 0$ the sum of the left is

$$\sum_{k=0}^{0} \binom{n+k}{n} \frac{1}{2^k} = \binom{n}{n} \frac{1}{2^0} = 1$$

and the function on the right is $2^0 = 1$ establishing a basis for induction. Assume that

$$\sum_{k=0}^{n} \binom{n}{n+k} \frac{1}{2^k} = 2^n$$

for some $n \geq 0$. Recall Pascal's identity

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$$

Then

$$\sum_{k=0}^{n+1} \binom{n+1}{n+1+k} \frac{1}{2^k} = \sum_{k=0}^{n+1} \left( \binom{n}{n+1+k} + \binom{n}{n+k} \right) \frac{1}{2^k}$$