Section 1.4 Mathematical Proofs

1. **(Direct Proof)** Prove the following by a direct proof.

a) The sum of two even integers is even.

Ans: Let m,n be two even integers. Hence we can write $m = 2k_1, n = 2k_2$ where k_1, k_2 are integers. Thus the sum is $m+n = 2k_1 + 2k_2 = 2(k_1 + k_2) = 2k_3$ where k_3 is an integer.. In other words $m+n$ is 2 times an integer, which means $m+n$ is an even integer.

b) The sum of an even and odd integer is odd.

Ans: Let m be an even integer and n an odd integer. Hence, we can write $m = 2k_1$ and $n = 2k_2 + 1$ where k_1 and k_2 are integers. Thus we have the sum $m+n = 2k_1 + 2k_2 + 1 = 2(k_1 + k_2) + 1 = 2k_3 + 1$, where k_3 is an integer. In other words $m+n$ is of the form $2k_3 + 1$ which means it is an odd integer.

c) If a divides b, and b divides c, then a divides c.

Ans: If a divides b and b divides c, we have $b = k_1 a$ and $c = k_2 b$ where k_1 and k_2 are integers. Hence $c = k_2 b = k_2(k_1 a) = (k_1 k_2) a = k_3 a$ where $k_3 = k_1 k_2$ is an integer. Hence, a divides c.

d) The product of two consecutive natural numbers plus the larger number is a perfect square.

Ans: Let $n, n+1$ be two consecutive natural numbers. Hence, the product of two consecutive natural numbers plus the larger number is

$$n(n+1) + n + 1 = (n+1)(n+1) = (n+1)^2$$

which means it is a perfect square.

e) Every odd integer n greater than 1 can be written as the difference between two perfect squares. Give examples for a few such integers.

Ans: Since $n > 1$ we know it can be written as the product $n = n_1 n_2$, where n_1, n_2 are odd positive integers, where we assume $n_1 > n_2$. Hence, we can write

$$n_1 n_2 = \left(\frac{n_1 + n_2}{2}\right)^2 - \left(\frac{n_1 - n_2}{2}\right)^2$$

and since both n_1, n_2 are both odd, $n_1 + n_2$ and $n_1 - n_2$ are both even integers, and hence

$$\frac{n_1 + n_2}{2}, \frac{n_1 - n_2}{2}$$

are integers, which proves the result. Some examples are $3 = 2^2 - 1^2, 5 = 3^2 - 2^2, 7 = 4^2 - 3^2, \ldots$.

b) If n is an even positive integer, then n is the difference of two positive integer squares if and only if $n = 4k$ for some integer $k > 1$.

Ans: $(\Rightarrow)$ Let $n = a^2 - b^2 = (a+b)(a-b)$ be an even positive integer where $a > b$ are positive integers. Letting $n_1 = a+b,\ n_2 = a-b$ so we have

$$a = \frac{n_1 + n_2}{2},\ b = \frac{n_1 - n_2}{2}.$$

Now since a, b are integers, then n_1, n_2 are both odd or both even. They can not both be odd since by assumption n is even. Hence, for some integers k_1, k_2 where $k_1 > k_2$, $n_1 = 2k_1,\ n_2 = 2k_2$. Therefore, we have $n = n_1 n_2 = 4k_1 k_2 = 4k$, $k > 1$, which proves the result.

$(\Leftarrow)$ We assume $n = 4k$ for some integer $k > 1$. Hence $k = k_1 k_2$ for positive integers k_1, k_2 where $k_1 > k_2$. Therefore $n = 4k = 4k_1 k_1 = (k_1 + k_2)^2 - (k_1 - k_2)^2$ which proves the result.

f) If a, b are real numbers, then $a^2 + b^2 \geq 2ab.$

Ans: We know $a^2 - 2ab + b^2 = (a-b)^2 \geq 0$ and so $a^2 + b^2 \geq 2ab.$

g) The sum of two rational numbers is rational.

Ans: **Let** $m = p/q,\ n = r/s$ be rational numbers where p, q, r, s are integers with q, s nonzero.

Hence, their sum is $m + n = \frac{p}{q} + \frac{r}{s} = \frac{ps + qr}{qs}$ which is a rational number.

h) Let $p(x)$ be a polynomial and E is the sum of the coefficients of the even powers, and O the sum of the coefficients of the odd powers. Show $E + O = p(1)$ and $E - O = p(-1)$.

Ans: Case 1: Let $p(x)$ be an even polynomial and write $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$

where n is an even positive integer. Hence,

$$E = a_n + a_{n-2} + \cdots + a_0$$
$$O = a_{n-1} + a_{n-3} + \cdots + a_1$$

Hence

$$\begin{aligned} E - O &= (a_n + a_{n-2} + \cdots + a_0) - (a_{n-1} + a_{n-3} + \cdots + a_1) \\ &= a_n - a_{n-1} + a_{n-2} - a_{n-3} + \cdots + a_1 - a_0 \\ &= p(-1) \end{aligned}$$

$$\begin{aligned} E + O &= (a_n + a_{n-2} + \cdots + a_0) + (a_{n-1} + a_{n-3} + \cdots + a_1) \\ &= a_n + a_{n-1} + a_{n-2} + \cdots + a_1 + a_0 \\ &= p(1) \end{aligned}$$

The case of an odd polynomial follows along the same lines.

2. **(Divisibility by 4)** Show that a natural number is divisible by 4 if and only if its last two digits are. For example 4 divides 256 and also divides 56.

Ans: We can write any natural number n in the form $n = q(100) + s(10) + r$ where q, r, s are natural numbers where $0 \le s \le 9$ is the digit in the one's place and $0 \le s \le 9$ is the digit in the 10's place (For example $354092 = 3540(100) + 9(10) + 2$ where $s = 9, r = 2$.) Now, since 4 divides 100 we know that 4 divides n if and only if it divides $10s + r$, which are the last two digits of n.

3. **(Divisibility by 3**) Show that a natural number is divisible by 3 if and only if the sum of its digits is divisible by 3.

Ans: Sometimes it is instructive to see how the argument goes for a specific number. For example consider the number $n = 2856$ where we want to see why 3 divides 2856 if and only if 3 divides $2 + 8 + 5 + 6$. The proof uses the fact that when any power of 10 is divided by 3, the remainder is always 1 as in

$$\begin{aligned} 10 &= 3 \cdot 3 + 1 \\ 100 &= 33 \cdot 3 + 1 \\ 1000 &= 333 \cdot 3 + 1 \end{aligned}$$

and so on. Hence, performing a little creative arithmetic, we can write our number as

$$\begin{aligned} 2856 &= 2(1000) + 8(100) + 5(10) + 6 \\ &= 2(333 \cdot 3 + 1) + 8(33 \cdot 3 + 1) + 5(3 \cdot 3 + 1) + 6 \\ &= (2 \cdot 333 \cdot 3 + 2 \cdot 1) + (8 \cdot 33 \cdot 3 + 8 \cdot 1) + (5 \cdot 3 \cdot 3 + 5 \cdot 1) + 6 \\ &= (2 \cdot 333 + 8 \cdot 33 + 5 \cdot 3) \cdot 3 + (2 + 8 + 5 + 6) \end{aligned}$$

But clearly 3 divides the first term $(2\cdot 333+8\cdot 33+5\cdot 3)\cdot 3$ and so 3 divides 2856 if and only if it divide the sum of its digits $2+8+5+6$. The general proof would carry out these steps in a more general setting, but the idea is the same. Note: A similar proof can be used to show that any natural number is divisible by 9 if and only if 9 divides the sum of the digits of the number.

4. **(Proof by Contradiction)** Prove the following by contradiction

a) If n is an integer and $5n+2$ is an even integer, then n is even.

Ans: We assume that n is an integer where $5n+2$ is an even integer, but that n is odd. Hence we can write $n=2k+1$ where k is an integer, and so $5n+2=5(2k+1)+2=10k+7$ which is odd and contradicts the assumption that $5n+2$ is even.

b) If x and y are integers and $x+y$ is even, then x and y have the same parity (i.e. both are even or both are odd).

Ans:

c) Let x and y be integers. If xy is even, then at least one of x and y must be even.

Ans:

d) I is an irrational number and R is a rational number, then $I+R$ is irrational.

Ans: We write $R=p/q$ $(q\neq 0)$ and assume that $I+R$ is a rational number, say $I+R=P/Q$ $(Q\neq 0)$. Hence we have

$$I+\frac{p}{q}=\frac{P}{Q}\Rightarrow I=\frac{P}{Q}-\frac{p}{q}=\frac{Pq-Qp}{Qq}$$

which contradicts the fact that I is irrational. Hence, $I+R$ is irrational.

5. **(Divisibility Problem)** Prove the following theorems for integers $m,n.$.

a) 5 divides n^4-1 if and only if 5 does not divide n.
Ans: Reader's choice

b) 9 divides n if and only if 9 divides the sum of the digits of n.
Ans: Reader's choice

c) The produce mn is even if and only if at least one of m and n is even.
Ans: Reader's choice

6. **(Counterexamples)** A counterexample is an exception to a rule. In mathematics, they are used to probe the boundaries of a theorem. A counterexample[1] to a given claim may show that the assumptions are false or incomplete, and thus allow the mathematician to add or adjust the conjectures. Find counterexamples for the following faulty theorems and tell how you could add new hypothesis to make the claim valid.

a) If $a > b$ then $|a| > |b|$.

Ans: Let $a = 1, b = -2$. Here $a > b$ but $|a| = 1, |b| = 2$ and so $|a| < |b|$. If we add the assumption that a, b are nonnegative real numbers, then the result holds.

b) If $(a-b)^2 = (m-n)^2$ then $a-b = m-n$.

Ans: If $a = 2, b = 1, m = 1, n = 2$, then $(a-b)^2 = (m-n)^2 = 1$ but $a-b = 1$ and $m-n = -1$. If we add the assumption that $a > b, m > n$ then the result holds.

c) If x and y are real numbers, then $\sqrt{xy} = \sqrt{x}\sqrt{y}$.

Ans: Let $x = -1, y = -1$, then $\sqrt{xy} = \sqrt{(-1)(-1)} = \sqrt{1} = 1$ but $\sqrt{-1}\ \sqrt{-1} = i^2 = -1$. If we add the assumption that both x, y are nonnegative the result holds.

d) If f is a continuous real-valued function defined on $[a,b]$, then there exists a $c \in (a,b)$ such that

$$f'(c) = \frac{f(b) - f(a)}{b-a}$$

Ans: Let $f(x) = |x|$ and $a = -1, b = 1$. Here

$$\frac{f(b) - f(a)}{b-a} = \frac{f(1) - f(-1)}{2} = 0$$

but the derivative of f is

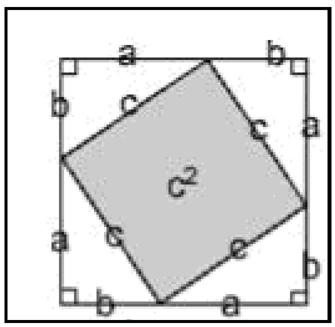
$$f'(x) = \begin{cases} -1 & -1 < x < 0 \\ \text{does not exist} & x = 0 \\ 1 & 0 < x < 1 \end{cases}$$

Hence, the derivative is never 0 on the interval $(a,b) = (-1,1)$. If we add the extra condition that f is differentiable on (a,b), then the result holds. This, of course, is the mean value theorem from calculus.

[1] A nice reference book for any mathematician is *Counterexamples in Mathematics* by Bernard Geldbaum and John Olmsted, Springer-Verlag (1990).

7. **(Valid Proof – Invalid Conclusion)** Keep in mind a proof of a theorem can be valid but the conclusion false if the assumptions of the theorem are false. For example, assuming the existence of a largest positive integer N (clearly false), prove the false statement $N = 1$.
Ans: Assuming the contrary that $N > 1$, we have $N^2 > N$. But we have assumed N is the largest positive integer and hence $N > N^2$. Therefore $N = N^2$ which implies $N = 1$.
Note: We have proven a theorem of the form $P \Rightarrow Q$ by proving its equivalent form $(P \wedge \sim Q) \Rightarrow Q$.

8. **(Pythagorean Theorem)** Prove the Pythagorean Theorem. That is, if a, b, c are the sides of a right triangle where c is the hypotenuse, then $a^2 + b^2 = c^2$. Use the diagram in the following figure and set the area of the larger square equal to the sum of the sub-triangles and square inside it.



Visual Proof of the Pythagorean Theorem

Ans: The area of the larger square is $(a+b)^2 = a^2 + 2ab + b^2$. The area of the smaller square is c^2 and the total area of the four triangles is

$$4\left(\frac{1}{2}ab\right) = 2ab.$$

Setting the area of the larger square equal to the smaller square plus the four triangles, gives $a^2 + 2ab + b^2 = c^2 + 2ab$, which after simplifying gives the Pythagorean Theorem $a^2 + b^2 = c^2$.

9. **Comparing Theorems** Verify the statement

$$(J \Rightarrow S) \Rightarrow \left[(S \Rightarrow C) \Rightarrow (J \Rightarrow C)\right]$$

which shows the theorem $S \Rightarrow C$ (with the weaker hypothesis) is a stronger theorem than $J \Rightarrow C$.
Ans: Constructing a truth table we see we have all T's in column (5), and so the statement is a tautology.

			(1)	(2)	(3)	(4)	(5)
J	S	C	$J \Rightarrow S$	$S \Rightarrow C$	$J \Rightarrow C$	$(S \Rightarrow C) \Rightarrow (J \Rightarrow C)$	$(J \Rightarrow S) \Rightarrow [(S \Rightarrow C) \Rightarrow (J \Rightarrow C)]$
T	T	T	T	T	T	T	**T**
T	T	F	T	F	F	T	**T**
T	F	T	F	T	T	T	**T**
T	F	F	F	T	F	F	**T**
F	T	T	T	T	T	T	**T**
F	T	F	T	F	T	T	**T**
F	F	T	T	T	T	T	**T**
F	F	F	T	T	T	T	**T**

10. **Comparing Theorems** Verify that theorem $J \Rightarrow C_1$ is stronger (implies) than theorem $J \Rightarrow C_2$ if conclusion C_1 is stronger than conclusion C_2. In other words show that

$$(C_1 \Rightarrow C_2) \Rightarrow [(J \Rightarrow C_1) \Rightarrow (J \Rightarrow C_2)]$$

is a tautology. This means if two theorems have the same hypothesis, then the theorem with the stronger conclusion is superior.

Ans: Constructing a truth table we see we have all T's in column (5), and so the statement is a tautology

			(1)	(2)	(3)	(4)	(5)
J	C_1	C_2	$J \Rightarrow C_1$	$J \Rightarrow C_2$	$C_1 \Rightarrow C_2$	$(J \Rightarrow C_1) \Rightarrow (J \Rightarrow C_2)$	$(C_1 \Rightarrow C_2) \Rightarrow [(J \Rightarrow C_1) \Rightarrow (J \Rightarrow C_2)]$
T	T	T	T	T	T	T	**T**
T	T	F	T	F	F	F	**T**
T	F	T	F	T	T	T	**T**
T	F	F	F	F	T	T	**T**
F	T	T	T	T	T	T	**T**
F	T	F	T	T	F	T	**T**
F	F	T	T	T	T	T	**T**
F	F	F	T	T	T	T	**T**

11. **(Proof that** $1 = 0.999...$) Infinite decimals are needed to represent certain fractions. Using long division the fraction 1/3 is represented in decimal form as $1/3 = 0.333....$ .Show that this representation yields a proof that $1 = 0.999...$ by writing

$$1 = 3 \cdot \left(\frac{1}{3}\right).$$

There are other proofs as well. Can you find some?

Ans: The repeating decimal 0.999… (or sometimes written $0.\overline{9}$) denotes the number 1. There are various proofs of varying degrees of rigor to show that this quantity is 1. A common proof is to let $x = 0.999\ldots$ and so $10x = 9.999\ldots$ and subtracting, yields $10x - x = 9.999\ldots - 0.999\ldots = 9$ or $9x = 9$ or $x = 1$.

d) Prove that 1 is equal to 0.9999 ….

Ans: Write

$$\begin{aligned} 0.999\ldots &= \frac{9}{10} + \frac{9}{100} + \frac{9}{1000} + \cdots \\ &= \frac{9}{10}\left[1 + \frac{1}{10} + \left(\frac{1}{10}\right)^2 + \cdots\right] \\ &= \frac{9}{10}\left(\frac{1}{1-(1/10)}\right) \\ &= \frac{9}{10}\left(\frac{10}{9}\right) = 1 \end{aligned}$$

12. **(Analysis of the Structure of Proofs)** There is a theorem in mathematics that states that a compact set is both closed and bounded. A common way to prove this theorem is my contrapositive which would say if it is not true that a set is both closed and bounded then the set is not compact. Using DeMorgan's law one could restate this by stating

If a set is not closed or not bounded then the set is not compact.

How would you go about proving this statement ?

Ans: From the tautology

$$\left[\left(\sim P \vee \sim Q\right) \Rightarrow R\right] \equiv \left[\left(\sim P \Rightarrow R\right) \wedge \left(\sim Q \Rightarrow R\right)\right]$$

the proof proceeds by assuming the set is not closed and proving the set compact, and then assuming the set is not bounded and proving the set is not compact.

13. **(Another Irrational Number)** Prove that $\log_{10} 3$ is irrational.

Ans: Assume the contrary; that is $\log_{10} 3 = p/q$. By the definition of the logarithm, we have $10^{p/q} = 3$ where p and q are positive integers. Hence, we have $10^m = 3^n$. But this is impossible since for every positive power 10^p is even and 3^q is odd.

14. **(Not Proofs)** The following are not considered valid proofs by most mathematicians. Maybe the reader knows of a few other ones.

- Proof by obviousness: The proof is so clear that it need not be mentioned.
- Proof by plausibility: It sounds good, so it must be true.
- Proof by intimidation: Don't be stupid; of course it's true!
- Proof by definition: I define it to be true.
- Proof by tautology: It's true because it's true.
- Proof by majority rule: Everyone I know says its true.
- Proof by divine word: ...and the Lord said, 'Let it be true' and it was true.
- Proof by hopeful generalization: Well, it works for 13, that's enough for me.
- Proof by hope: Please, let it be true.
- Proof by intuition: I just have this feeling.

15. **(Just a Little Common Sense)** You are given a column of 100 ten-digit numbers and after adding them you get an answer of 2437507464567. Is your answer correct ?
Ans: Your answer has 13 digits in it but the largest the sum of 100 ten-digit numbers can be is $9999999999 \times 100 = 999999999999$ which is a ten-digit numbers. Hence, your answer can not be correct.

16. **(Syllogisms)** The Greek philosopher Plato is generally recognized as the first person associated with the concept a logical argument, which took the form of two premises followed by a conclusion. This basic logical form is called a **syllogism**, the most famous being the "Socrates syllogism":

First premise: *All men are mortal,*
Second premise: *Socrates is a man,*
Conclusion: *Therefore, Socrates is mortal.*

which has the general form

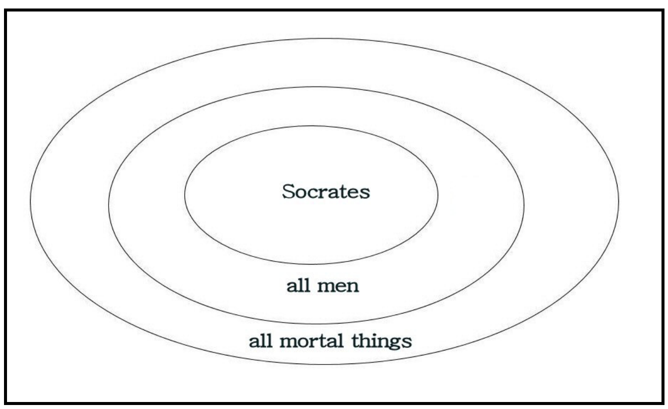
First premise: M - P
Second premise: $S - M$
Conclusion: $S - P$

where $S =$ "being Socrates" and $P =$ "being mortal" are called the **subject** and **predicate** of the syllogism, and $M =$ "being man" is called the **middle term** of the syllogism.

Plato classified each premise and conclusion as one of the four basic types[2]:

E: Every A is B (example: Every dog has a tail)
S: Some A is B (example: Some dogs have black hair)
N: No A is B (example: No dog has orange hair)
Sn: Some A are not B (example: Some dogs are not poodles)

which means there are a possible total of $4\times4\times4 = 64$ possible syllogisms, some logically true, some false. We would denote the Socrates syllogism by EEE, meaning each of the 2 premises and conclusion in the syllogism are of type E. To convince yourself that this syllogism is logically valid, we draw the following Venn diagram where we would argue that if the set of "all men" is inside the set of "all mortal things" and if Socrates is inside the collection of "all men," then surely Socrates is inside the set of "all mortal things."



Of the 16 possible syllogisms, 4 are logically valid and 12 are invalid. Which of the following syllogisms are valid and which are invalid? Draw Venn diagrams to support your argument.

a) NEN **Ans:** true
b) ESS **Ans:** true
c) NSSn **Ans:** true
d) SSS **Ans:** false
e) EES **Ans:** false
f) SES **Ans:** false

---

[2] We use A and B to denote the properties S, P, and M.

17. **(Euler's Totient Function)** Euler's totient function, denoted by $\phi(n)$, gives the number of natural numbers less than a given natural number n, including 1, that are relatively prime to n, where two numbers are relatively prime if their greatest common divisor is 1. For example $\phi(p) = p-1$ for any prime number since $1,2,3,\ldots,p-1$ are all relatively prime with p. On the other hand $\phi(12) = 4$ since 1, 5, 7, and 11 are relatively prime with 12. Prove that for a power of a prime number $p^k, k = 1,2,\ldots$ the Euler totient function is $\phi(p^k) = p^{k-1}(p-1)$ by proving

a) Find the number of natural numbers strictly between 1 and p^k that are not relatively prime with p^k; i.e. divide p^k.
b) Subtract the result from a) from $p^k - 1$ to obtain $\phi(p^k)$
Ans: The numbers between 1 and p^k that have a common factor with p^k *greater than one* are $p, 2p, 3p, \ldots, (p^{k-1}-1)p$ which give a total of $p^{k-1}-1$. Hence the number of natural numbers less than p^k relatively prime with p^k is the difference

18.(**Pick's Amazing Formula**) In 1899 an Austrian mathematician, Georg Pick devised a fastinating formula for finding the area A inside a simple polygon whose vertices lie on grid points (m,n) where m and n are integers. By a unit area we mean the area of a simple square bounded by four vertices, and by a simple polygon we mean that the polygon has no "holes" in it and that the edges do not intersect. The formula he came up with was

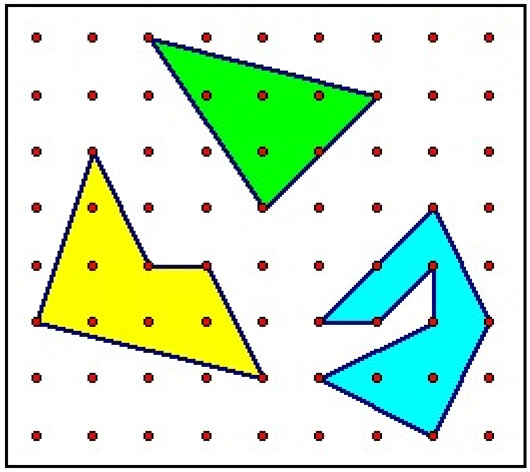
$$A = \frac{B}{2} + I - 1$$

where B is the number of vertices that lie on the boundary of the polygon, and I is the number of vertices that lie interior to the polygon.

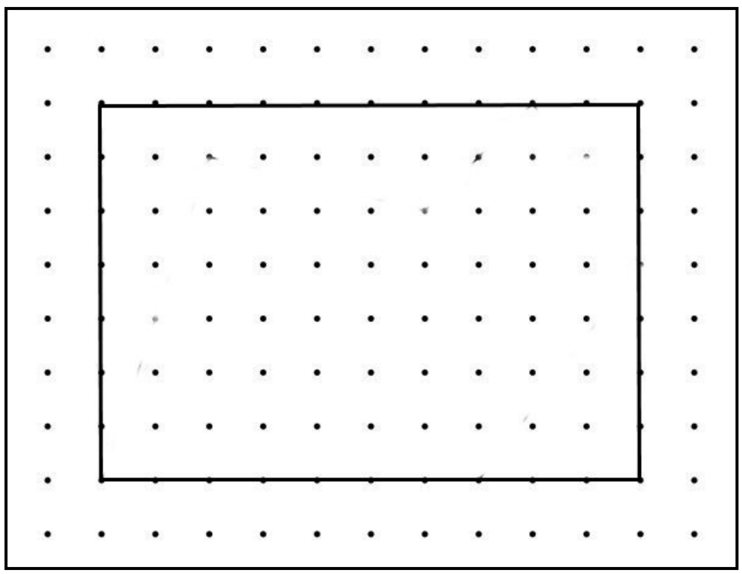
a) Verify that Pick's formula yields an area of 1 for a simple square bounded by four vertices.

b) Use Pick's formula to find the area inside the polygons in Figure 1.

c) Prove that Pick's formula yields the correct solution for finding the area of a rectangle with m rows and n columns. We draw a $m = 7$ by $n = 10$ rectangle in the following figures for illustration.



Applying Pick's Formula



Verifying the Area mn of an $m \times n$ Rectangle

Ans:

a) For a simple square bounded by four vertices, we have $B = 4,\ I = 0$ for an inside area of

$$A = \frac{4}{2} + 0 - 1 = 1 \text{ square unit}$$

b) For the triangle we have $B = 4,\ I = 4$, so the area inside is

$$A = \frac{4}{2} + 4 - 1 = 5 \text{ square units}$$

For the polygon with 5 sides, we have $B = 5,\ I = 5$ and so the area is

$$A = \frac{5}{2} + 5 - 1 = 6.5 \text{ square units}$$

For the polygon with 85 sides, we have $B = 9,\ I = 2$ and so the area is

$$A = \frac{9}{2} + 2 - 1 = 5.5 \text{ square units}$$

c) The number of boundary points for an $m \times n$ rectangle is $B = 2m + 2n$ and the number of interior points is $I = (m-1)(n-1)$ so Pick's formula yields the interior area as

$$\begin{aligned} A &= \frac{2m+2n}{2} + (m-1)(n-1) - 1 \\ &= \frac{2m+2n+2mn-2n-2m}{2} \\ &= mn \end{aligned}$$

which is the area of an $m \times n$ rectangle. For example the rectangle in Figure 2 we have $m = 7$ by $n = 10$ and so it has area $mn = 70$ square units.

ΚΛΞΨΩΔΧ