SOME NOTES FOR THE MATHEMATICS PROBLEM GROUP

BARRY MONSON and DARYL TINGLEY
DEPARTMENT OF MATHEMATICS & STATISTICS
UNIVERSITY OF NEW BRUNSWICK

1 Terminology and Basic Ideas

A.**Notation for Numbers**:

$$\mathbb{N} \subset \mathbb{Q} \subset \mathbb{Z} \subset \mathbb{R} \subset \mathbb{C}$$

The previous statement summarizes neatly how certain sets of numbers are **subsets** of other sets of numbers. **Set theory** provides a very convenient and concise way of describing complicated mathematical relationships. For more on sets and how to use them, see § 8.

1. $\mathbb{N} = \{\text{natural numbers}\} = \{1,\ \ 2,\ \ 3,\ \ 4,\ \ \ldots\}$
   (a) Some people include 0 as a natural number,too.
   (b) a natural number $n > 1$ is prime if (like 13) it has no positive divisors other than 1 and n itself. Otherwise n is composite, like 14, which has the positive divisors $1, 2, 7, 14$ (and negative divisors $-1, -2, -7, -14$, too).
2. $\mathbb{Z} = \{\text{integers}\} = \{\ldots,\ \ -3,\ \ -2,\ \ -1,\ \ 0,\ \ 1,\ \ 2,\ \ \ldots\}$
3. $\mathbb{Q} = \{\text{rationals}\} = \left\{ \frac{m}{n} \middle| m,\ \ n \in \mathbb{Z}\ \text{ with }\ n \neq 0 \right\}$
   (a) e.g. $0 = \frac{0}{3},\ \ -\frac{2}{3},\ \ 17.31 = \frac{1731}{100}$, etc.
4. $\mathbb{R} = \{\text{all real numbers}\}$
   (a) Real numbers x correspond exactly to the points on a line.
   (b) Thus $\frac{2}{3}$ is real. But "most" reals are irrational – like $\sqrt{2}$, they cannot be written as a ratio of integers. Other irrationals are $\sqrt{p}$, if p is any prime; the very special irrational numbers π and e are transcendental.
   (c) All reals have "infinite" decimal expansions, but only those for rationals eventually have a block of digits which repeats forever.
   E.g. $13 = 13.\underline{0}00$ ... (we could think of the "0" as a block of length one which repeats forever).
   Here is another, more typical, rational number:
   $$\frac{2047}{495} = 4.1\underline{35}3535\ldots \quad .$$
   But $\pi = 3.1415926\ldots$ has no such repeating block of digits. It is quite tricky to prove that π is irrational.

(d) The **greatest integer or floor function**: for any real number x, we look at

$$\begin{aligned} \lfloor x \rfloor &= \text{floor of } x \\ &= \text{greatest integer in } x \\ &= \text{greatest integer not exceeding } x. \end{aligned}$$

Thus

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1.$$

Here are some examples:

$$\begin{aligned} \lfloor 3.1 \rfloor &= 3 \\ \lfloor 4 \rfloor &= 4 \\ \lfloor -0.2 \rfloor &= -1. \end{aligned}$$

We will look at the **ceiling** below.

5. $\mathbb{C} = \{\text{complex numbers}\} = \{x + yi \mid x, y \ \epsilon \ \mathbb{R}\}$.

   (a) Here $i^2 = -1$.

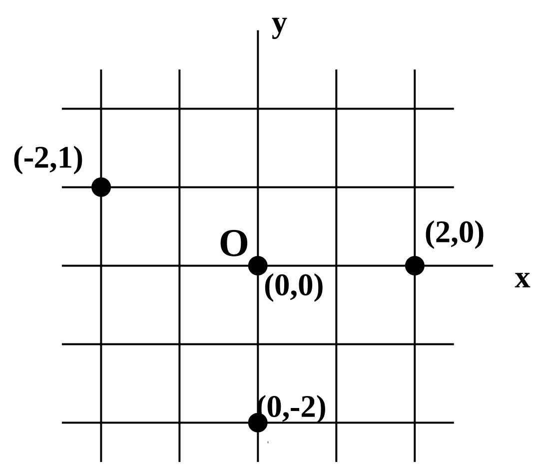
   (b) Complex numbers z correspond to the points in a plane.

2 Euclidean Spaces.

1. Points on a straight line are described by a single real number x (which is called a coordinate).
2. Points in a plane are described by an ordered pair (x, y) of reals.
   (a) We thus denote the plane as
   $$\mathbb{R}^2 = \{(x, y) \mid x \;\; y \;\; \epsilon \;\; \mathbb{R}\}.$$
   (b) Points in the plane may also be described by one complex number w, instead of two reals $x, \;\; y$.
3. In solving geometry problems analytically we use tricky algebraic manipulation of coordinates.

   The synthetic approach avoids coordinates and uses instead congruence, angles and various Euclidean theorems.

   A given problem may be hopeless using one approach, easy using the other. Perhaps a "combined assault" will work best.
4. The unit lattice Z^2 is the set of points in the plane with integer coordinates. These points form a grid of unit squares which tessellate the plane.



5. Points in ordinary space $\mathbb{R}^3$ are described by ordered triples (x, y, z) of reals. We can do solid geometry problems analytically (or synthetically).
6. Even more recklessly we can do geometry in 4-dimensional space $\mathbb{R}^4$ using (x, y, z, v) to represent one point. Though it is difficult to visualize such figures, there are many practical "non-visual" applications.

3 The Pigeonhole Principle.

A. 1. The ceiling: for any real number x

$$\lceil x \rceil = \text{ceiling of } x = \text{smallest integer not less than } x$$

so:

$$\lceil x \rceil - 1 < x \leq \lceil x \rceil$$

e.g.:

$$\begin{array}{ll} \lceil 3 \rceil = 3, & \lceil 3.1 \rceil = 4, \\ \lceil -2 \rceil = -2, & \lceil -.9 \rceil = 0. \end{array}$$

2. The Pigeonhole Principle

   If you put $p+1$ pigeons into p holes then some hole contains at least 2 pigeons

   – or more generally –

   if you put w widgits into b boxes, then some box contains at least $\lceil w/b \rceil$ widgits.

   Proof: by contradiction.

B. Try some problems. They aren't necessarily easy! To use the pigeon hole principle, you need only decide: What are the pigeons? What are the holes?

1. In any party with n people ($n \geq 2$) show that at least two have the same number of acquaintances.
2. Prove that in a group of 13 people at least two have their birthdays in the same month.
3. Take any six points in the plane, no three of them on a line. Join all pairs of points by line segments, using a red or blue pencil. Show that you must have a triangle of one colour (Putnam-53).

   We might re-phrase this as the party problem: Prove that in a group of 6 people at a party, there are at least three people who mutually know each other or at least three who are mutual strangers.
4. Show, however, that there could be a group of 5 people such that no group of three mutually know each other and no group of three are mutual strangers.
5. Show that in the group of six party people, there are one of the following:

   (i) two groups of three who mutually know each other;

   (ii) two groups of three who mutually don't know each other;

   (iii) a group of three who do and a group of three who do not know each other.
6. How many times must we throw two dice in order to be sure that we get the same total score at least 6 times?

7. Show that given 17 numbers, it is possible to choose five whose sum is divisible by 5.
8. Pick any five points inside a unit square [a square of side 1]. Show that for at least one pair of points, the distance between the points is $\leq \frac{1}{\sqrt{2}}$ (Putnam-54).
9. Prove that of any 10 points chosen within an equilateral triangle of side length 1, there are two whose distance apart is at most $\frac{1}{3}$.
10. Let there be given nine lattice points (points with integral coordinates) in three dimensional Euclidean space. Show that there is a lattice point on the interior of one of the line segments joining two of these points (Putnam-71).
11. Pick any nine points in a unit square. Show that some three of these points form a triangle whose area is $\leq \frac{1}{8}$ unit.
12. Suppose that 70 different students are studying 11 different subjects and that any subject is studied by at most 15 students. Show that there are at least 3 subjects which are studied by at least 5 students each.

    The remaining problems may be even trickier!
13. Show, that in a rectangle measuring 197 by 94, we cannot place 24,000 points in such a way that no two points are less than 1 unit apart.
14. In a unit square, we draw a non self-intersecting curve consisting of straight segments of total length greater than $2n$. Prove that there is a line parallel to one of the sides of the square which intersects the zig-zag curve in at least $n + 1$ points.
15. Chose any integer n. Show that there is a multiple of n, this multiple containing only the digits 0 and 1 in its decimal expansion.
16. Given $n + 1$ positive integers, none exceeding $2n$; show that at least one of them divides another.

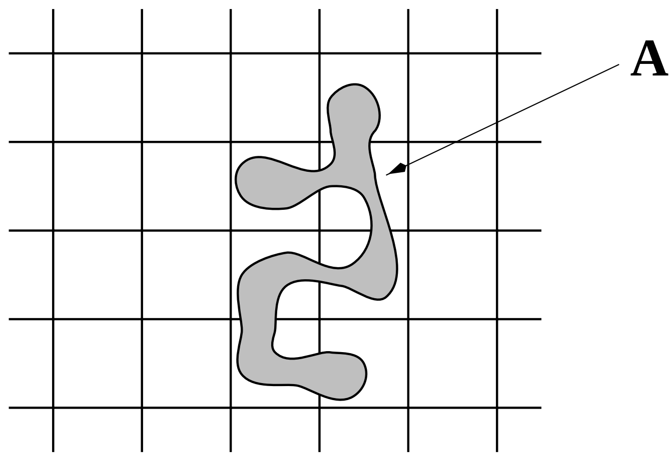
17. Recall that the unit lattice is the set of all points in the xy-plane with integer coordinates.

(a) Does every line through the origin pass through at least one other lattice point?

(b) Suppose a plane region has area A, and define the positive integer n by

$$n - 1 < A \leq n \, .$$

(Recall that we write $n = \lceil A \rceil$). Show that A can be shifted so as to cover at least n lattice points.



4 Some Techniques for Solving Problems Involving Integers

1. Mathematical Induction.
2. Divisibility arguments, greatest common divisors (GCD), least common multiples (LCM), primes, relatively prime.

Notation: (a, b) is the GCD of a and b. $a|b$ means "a divides b" (with no remainder).

Theorem (Euclid). There are infinitely many primes.

Theorem (Euclid). If $(a, b) = 1$ and $a|cb$ then $a|c$.

Theorem (Fundamental Theorem of Arithmetic). Every natural number (positive integer) can be uniquely written as

$$n = \prod_{p|n} p^{e_p}$$

where e_p is the largest number such that $p^{e_p}|n$.

Theorem (Division Algorithm). If n and d are positive integers then there are unique integers q and r such that

$$n = qd + r \quad \text{, with} \quad 0 \leq r < d \; .$$

As a division, we customarily write

$$\frac{n}{d} = q + \frac{r}{d} \; .$$

Note furthermore that

$$(n, d) = (d, r) \; .$$

To see this second part, observe that if $p|n$ and $p|d$, then $p|(n - qd)$, i.e. $p|r$ also. If $p|d$ and $p|r$ then $p|(qd + r)$, i.e. $p|n$ also.

Some Problems

1. (Bernoulli's inequality) Show that for every $x > -1$ and every natural number n,

$$(1 + x)^n \geq 1 + nx.$$

2. The Fibonacci sequence is defined by $F_1 = 1$, $F_2 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$. Show that for every n, $(F_n, F_{n+1}) = 1$.
3. Prove $F_1^2 + F_2^2 + \ldots + F_n^2 = F_n F_{n+1}$.
4. Find all natural numbers n for which $n^4 + 4$ is prime. (Hint: Factor.)
5. Show $(3n + 4, \; 2n + 3) = 1$ for every n. (Hint: Use Euclidean algorithm.)
6. Find all integer solutions to $5x + 7y = 1$.
   Hint: "Guess" one solution, and then find the rest. Introduce an integer variable k, and write $x = f(k)$ $y = g(k)$ as your list of solutions. Be sure x and y are integers whenevery k is!
   Note: Equations where we want only integer solutions one calls Diophantine equations.
7. (Very Easy!) Prove that $yx + 8y = 1$ has no integer solutions.

5 Congruence - a simple idea that is very powerful!

We write

$$a \equiv b \pmod{m}$$

if $m|(a-b)$.

We read this as ' a is congruent to b mod (or modulo) m'.

We can do perfectly sensible arithmetic mod m, although each statement we make now has a new, and often useful, meaning:

(i) If $a \equiv b \pmod{m}$) and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$; and $ac \equiv bd \pmod{m}$). That is, congruences may be added and multiplied. Division is not always so nice.

(ii) Suppose $ab \equiv ac \pmod{m}$ and $(a, m) = 1$ (i.e. a and m are **relatively prime**). Then $b \equiv c \pmod{m}$. Furthermore if $(a, m) = 1$, then there exists an integer x with $ax \equiv 1 \pmod{m}$.

The arithmetic situation for division of this sort is particularly nice when m is *prime*.

(iii) If p is prime and a is any integer, then there is a integer b such that $a \cdot b \equiv 1 \pmod{p}$. In fact, b is *unique* $\pmod{p}$.

We write $b \equiv \dfrac{1}{a} \pmod{p}$) or $b = a^{-1} \pmod{p}$.

In mathematical language, the above show that the classes of equivalent integers $\pmod{p}$ (where p is prime) constitute a <u>finite field</u>. This means that arithmetic $\pmod{p}$) works just like ordinary arithmetic.

Fermat's Little Theorem.

If p is prime and p does not divide a, then $a^{p-1} \equiv 1 \pmod{p}$. Thus, always $a^p \equiv \pmod{p}$.

<u>**Problems**</u>

1. (Hard) Find the smallest integer n such that $47|2^n - 1$.
2. (Easy) Show $1^{241} + 2^{241} + 3^{241} + 4^{241}$ is divisible by 5.
3. Prove $20^{15} - 1$ is divisible by $11 \cdot 31 \cdot 61$.
4. Prove: $\sum_{i=1}^{6} i^n \equiv 0 \pmod{7}$ if and only if $n \equiv 0 \pmod{6}$.
5. Find the last three digits of 13^{398}.
6. Find the smallest natural number N such that
   (i) its decimal representation has 6 as the last digit;
   (ii) if the last digit is removed and placed in front of the remaining digits the resulting number is $4N$.
7. Find all n and k so that $(k+1)^n + \ldots + (k+5)^n$ is divisible by 5.

6 Key Ideas on Power Series.

A. Power Series with Centre a

$$\sum_{n=0}^{\infty} a_n (t-a)^n .$$

1. Let $x = t - a$; we get a function

   ** $$f(x) = \sum_{n=0}^{\infty} a_n x^n \quad , \qquad x \;\epsilon\; \mathbb{R} \; ,$$

   assuming the right hand side converges. When does this happen? Certainly

   $$f(0) = a_0 + 0 + 0 \ldots = a_0 .$$

2. Convergence Theorem. For some R, with $0 \leq R \leq \infty$, the series **

   (a) converges (absolutely) if $|x| < R$
   (b) diverges if $|x| > R$
   (c) converges or diverges if $|x| = R$.

3. Remarks.

   (a) In fact,

   $$1/R = \lim_{n\to\infty} \sup \sqrt[n]{|a_n|} \; .$$

   (b) There are "easier" tests for the convergence of **, but they may not give a complete answer. Example:

   Ratio Tests for **

   If possible, compute $r = \lim_{n\to\infty} \left| \dfrac{a_{n+1} x^{n+1}}{a_n x^n} \right|$.

   If $r < 1$, absolute convergence
   $r > 1$, divergence
   $r = 1$, NO DECISION.

   (c) The above results hold word-for-word if we take x complex. Then ** converges inside a circle of radius R. In complex analysis it is very useful to allow n to be negative in **.

4. Manipulation of Series.

   For one or more power series (with x interior to all intervals of convergence) one can treat the series as you would finite sums: $+, -, \times, \div$, differentiate, integrate, etc.

B. EXAMPLES.

1. Geometric Series.

$(1-x)(1+x+\ldots+x^n) = 1-x^{n+1}$ (check!)

$$\sum_{n=0}^{\infty} x^n = 1+x+x^2+\ldots = \begin{cases} \frac{1}{1-x} & , \text{ if } |x|<1 \\ \text{diverges} & , \text{ if } |x|\geq 1 \end{cases}$$

(thus $R=1$).

Exercise. For $|r|<1$, compute

$$a+ar+ar^2+\ldots \quad .$$

2. Taylor-Maclaurin Series.

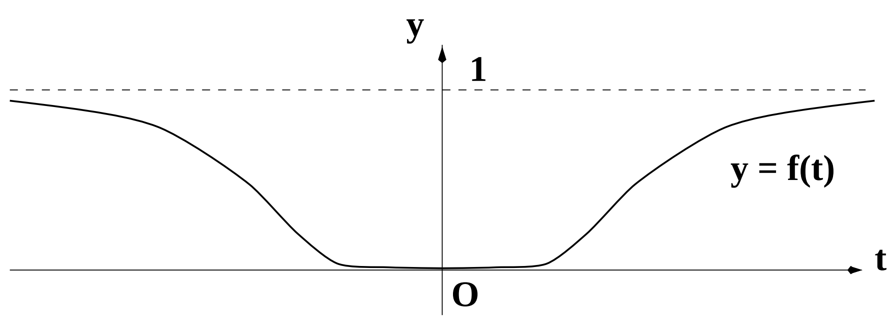
(a) Suppose a function $f(t)$ is C^∞ at $t=a$, (i.e. for all $n\geq 0$ it has an nth derivative $f^{(n)}(a)$; recall $f^{(0)}(a)=f(a)$).
The Taylor series for f is

$$\sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!}(t-a)^n.$$

(b) Example. It can happen that $f(t)$ does not equal this series outside the centre.

Eg.
$$f(t) = \begin{cases} e^{-1/t^2} & , \quad t\neq 0 \\ 0 & ; \quad t=0 \end{cases} .$$

Here $a=0$ (Maclaurin Series).
Then for all $n\geq 0$, $f^{(n)}(0)=0$ which means that $f(t)$ is very flat near 0:



Thus, $f(t)>0$ for $t\neq 0$, but $\displaystyle\sum_{n=0}^{\infty}\frac{f^{(n)}(0)}{n!}t^n \equiv 0$ always.

3. Some Convergent Taylor Series (centre $a=0$).

(a) $\dfrac{1}{1-t} = 1+t+t^2+\ldots$ $(R=1)$

(b) $e^t = 1 + t + \frac{t^2}{2} + \frac{t^3}{6} + \dots$

$= 1 + \frac{t}{1!} + \frac{t^2}{2!} + \frac{t^3}{3!} + \dots \qquad (R = \infty)$

(c) $\sin t = t - \frac{t^3}{3!} + \frac{t^5}{5!} - \frac{t^7}{7!} + \dots \qquad (R = \infty)$

(most other useful examples can be derived from these).

(d) Exercise. Find Taylor series ($a = 0$) (and radius of convergence) for cost, $\cosh t$, $\sinh t$, $1/1 + t^2$, $\ln(1 - t)$, $(1 + t)^{-2}$.

4. (a) General Binomial Coefficients.

Let $p \in \mathbb{R}$ and let k be a non-negative integer. Define

$$\left(\begin{array}{c} p \\ k \end{array} \right) = \frac{p(p-1)\dots(p-k_1)}{k(k-1)\dots 1}, \quad k \geq 1$$

(so there are k terms both top and bottom).

Also let $\left(\begin{array}{c} p \\ 0 \end{array} \right) = 1$.

Eg.

$$\binom{1/2}{4} = \frac{1/2(-1/2)(-3/2)(-5/2)}{4 \cdot 3 \cdot 2 \cdot 1} = \frac{-5}{128} .$$

(b) General Binomial Theorem (due to Newton).

For any power p and for $|t| < 1$, $(1 + t)^p = \sum_{k=0}^{\infty} \left(\begin{array}{c} p \\ k \end{array} \right) t^k$.

C. PROBLEMS.

1. Use the binomial theorem to estimate $\sqrt{1.01}$; check by calculator.

2. Check that $\frac{d}{dx}(e^x) = e^x$.

3. Find by long division the first few terms in the Maclaurin series for $\tan x$.

4. Find Maclaurin series for

$$(1 + t)^{-1/2}$$
$$(1 - t^2)^{-1/2}$$
$$\arcsin t.$$

5. Find, for $|x| < 1$, the series for:

(a) $\ln(1 - x) = -\int_0^x \frac{dt}{1 - t}$.

(b) $\ln(1 + x)$

(c) $\ln\left(\dfrac{1+x}{1-x}\right)$

(d) Using (c) we have an efficient way to compute logs to (say) 4 places. Compute

(i) $\ln 2 \qquad \left(\text{let } 2 = \dfrac{1+x}{1-x}\right)$

(ii) $\ln(1.5)$

(iii) $\ln(3) = \ln 2 + \ln(1.5)$.

6. Calculating π.

(a) Find (easily) the Maclaurin series for $\dfrac{1}{1+t^2}$.

(b) Do the same for $\arctan x = \displaystyle\int_0^x \frac{dt}{1+t^2} \qquad (|x| < 1)$.

(c) Let $\alpha = \arctan \dfrac{1}{5}$, $\beta = \arctan \dfrac{1}{239}$. Compute $\tan(4\alpha - \beta)$, and thus easily calculate π to 10 places.

D. GENERATING FUNCTIONS.

1. A Common Problem. Given a sequence $a_0, a_1, a_2, \ldots$, find a "formula" for the nth term. There are various methods:

(a) inspection and guessing (verified by induction)

(b) power series

(c) exponential series.

We'll try method (b) next.

2. Problem. Find a_n, the number of different ways to put n balls into 5 different boxes, leaving none empty.

Solution.

Let e_j = number of balls in the jth box.

We want a_n = number of solutions in integers to

$$e_1 + e_2 + e_3 + e_4 + e_5 = n \qquad\qquad (\text{all } e_j \geq 1).$$

So a_n is the number of ways to write

$$x^n = x^{e_1} x^{e_2} x^{e_3} x^{e_4} x^{e_5}$$

as a product of five positive powers of x. Thus a_n is the number of ways we get x^n after multiplying out (five times)

$$(x + x^2 + x^3 \ldots) \ldots (x + x^2 + x^3 + \ldots) \ .$$

So finally a_n is the coefficient of x^n in the generating function

$$\begin{aligned} f(x) &= [x + x^2 + x^3 + \dots]^5 \\ &= [x/1 - x]^5 = x^5(1-x)^{-5} \\ &= x^5 \sum_{k=0}^{\infty} \left(\begin{array}{c} -5 \\ k \end{array} \right) (-x)^k \\ &= x^5 + 5x^6 + 15x^2 + \dots \end{aligned}$$

Conclusion. $a_n = 0$ for $n \leq 4$ (why?!!) For $n \geq 5$, $a_n = (-1)^n \left(\begin{array}{c} -5 \\ n-5 \end{array} \right)$.

3. Problem. Find a formula for the Fibonacci numbers, here defined by setting

$$\begin{aligned} a_0 &= a_1 = 1, \\ a_{n+2} &= a_n + a_{n+1} \ . \end{aligned}$$

We thus obtain the sequence

1, 1, 2, 3, 5, 8, 13, 21, ...

(Hint: After finding $f(x) = \sum_{n=0}^{\infty} a_n x^n$, you will need to use partial fractions to get two geometric series which are then combined.)

7 Choices.

Combinatorics is the art of counting the same thing in two different ways.

A. Binomial Coefficients.

1. Def.

$$\binom{n}{k} = \text{number of ways to choose } k \text{ things from a population of } n$$
$$\text{(without regard to order).}$$
$$= \text{number of } k \text{ element subsets of an } n \text{ element set.}$$

2. If we do care about the order of our choices we have

   2nd choice

   1st choice kth choice

$$P(n,k) = n(n-1)\dots(n-k+1)$$

   ordered selections. These are called permutations.

3. If we disregard order, then

$$k! = k(k-1)\dots 2 \cdot 1$$

   ordered choices count for the same unordered choice. Thus,

$$* \qquad \binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k(k-1)\dots 1} \quad \begin{array}{l} \longleftarrow \; k \text{ terms starting at } n \\ \longleftarrow \; k \text{ terms starting at } k \end{array}$$

4. (a) $\binom{n}{0} = 1:$ there is only one way to choose no things from n. If we compare * just above, it makes sense to define a product of no terms at all to be 1.
   In particular, we should define

$$0! = 1.$$

   (b) Thus $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$

   (c) $\binom{n}{n} = 1:$ similarly.

5. (a) $\binom{n}{k} = \binom{n}{n-k}:$ taking k things is equivalent to throwing away $n-k$.

(b) $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$.

<u>Proof.</u> Instead of messy algebra, let's focus on one of the n things. Call it x. Any choice of k things either does or does not include x. If x is included, there are $\binom{n-1}{k-1}$ ways to choose the remaining $k-1$ things from $n-1$. If x is not included, there are $\binom{n-1}{k}$ ways of choosing k thins from $n-1$.

6. This gives

<u>PASCALS TRIANGLE</u>

$$\begin{array}{c} 0 \\ 0\ 1\ 0 \\ 0\ 1\ 1\ 0 \\ 0\ 1\ 2\ 1\ 0 \\ 0\ 1\ 3\ 3\ 1\ 0 \\ 0\ 1\ 4\ 6\ 4\ 1\ 0 \\ 0\ 1\ 5\ 10\ 10\ 5\ 1\ 0 \\ \vdots \qquad \vdots \qquad \vdots \end{array}$$

7. We can easily prove the BINOMIAL THEOREM for any positive integer n:

$$\begin{aligned} ** \qquad (1+x)^n &= \sum_{k=0}^{n} \binom{n}{k} x^k \\ &= \binom{n}{0} 1 + \binom{n}{1} x + \binom{n}{2} x^2 + \ldots + \binom{n}{n} x^n \\ &= 1 + nx + \frac{(n^2-n)}{2} x^2 + \ldots + x^n. \end{aligned}$$

8. <u>Some neat by-products of **.</u>

(a) Let $x = 1$: $\quad 2^n = \sum_{k=0}^{n} \binom{n}{k}$.

What does this mean in terms of choices? In terms of sets?

(b) Take the derivative of *:

$$n(1+x)^{n-1} = \sum_{k=0}^{n} \binom{n}{k} kx^{k-1}.$$

Take $x = 1$: $\quad n2^{n-1} = \sum_{k=1}^{n} \binom{n}{k} k.$

(Why need not this last sum start with $k = 0$?)

(c) Let $x = e^t$; take 2nd derivatives:

$$\begin{aligned}(1+e^t)^n &= \sum_{k=0}^{n} \binom{n}{k} e^{kt} \\ ne^{2t}(n+e^{-t})(1+e^t)^{n-2} &= \sum_{k=0}^{n} \binom{n}{k} k^2 e^{kt}.\end{aligned}$$

Set $t = 0$ (thus solving a 1962 Putnam problem):

$$\sum_{k=0}^{n} \binom{n}{k} k^2 = n(n+1)2^{n-2}.$$

8 An Introduction to Sets

8.1

(a) **What are sets?** It is impossible to say just *exactly what a set is* without getting into a vicious circle. So let's proceed intuitively: a **set** A is any collection of objects x, each of which is called an **element** of the set.

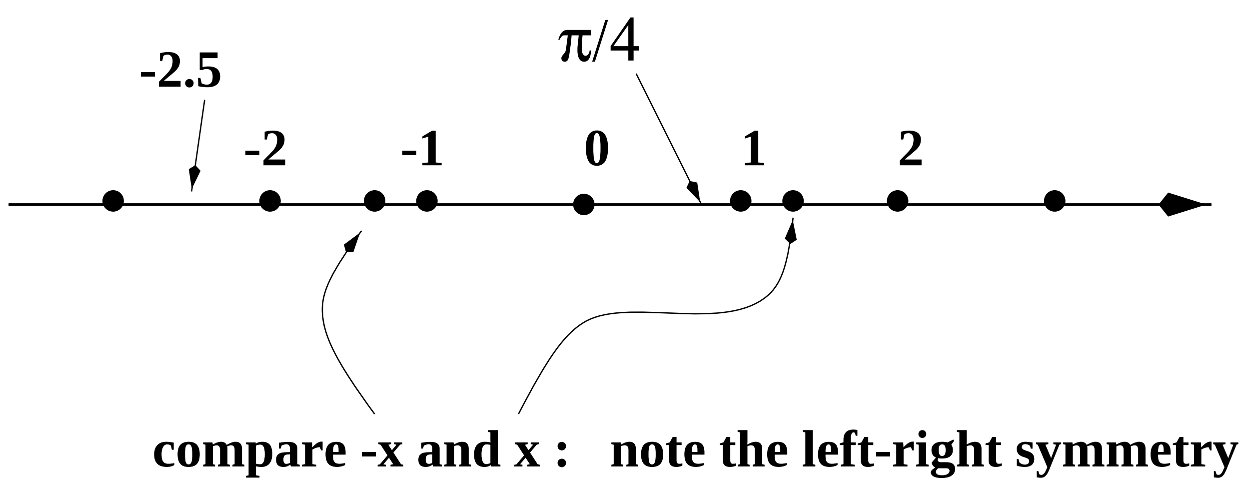
Typically curly braces { } are used to enclose the elements of the set. We write $x \in A$ if the object x happens to be an element of the set A; we also say that x is *in* A. If the object y is not in A, we write $y \notin A$.

(b) For example, we often work with **natural numbers**. The set of all natural numbers is denoted this way:

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\} \ .$$

thus, $1 \in \mathbb{N}$, $19935 \in \mathbb{N}$, but $-3 \notin \mathbb{N}$, $\frac{31}{10} \notin \mathbb{N}$, $\pi \notin \mathbb{N}$.

(c) Mind you, it will often be useful to work with the complete set $\mathbb{R}$ of **real numbers**, which correspond exactly to the points on a straight line:



Having selected an origin 0 and unit point 1, we can thereby place the natural numbers, the negative integers, the rational numbers, indeed all other real numbers x. You can see that $\mathbb{N}$ forms a very small portion of $\mathbb{R}$.

(d) The fact that the line extends infinitely far in *both* directions is the real reason that we have the set of **integers**

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} \ .$$

The diagram also suggest a simple counting rule. Suppose that k is an integer which is at most equal another integer n: so $k \leq n$. Geometry tells us that there are $n - k$ steps from k to n. Each step counts just one endpoint of a unit segment, say the right end. Thus the total endpoints are $n - k + 1$.

Interval Rule: If $k \leq n$, the total number of integers from k to n *inclusive* is $n - k + 1$.

8.2 Some Number Theory

(a) **Divisors and Modular Arithmetic:** here we shall review a little number theory, which concerns itself mainly with **integers**.

If $d, a \in \mathbb{Z}$, we say d **divides** a if $a = qd$ for some integer q, written

$$d \mid a \,.$$

We also say that d is a divisor of a, or that a is a **multiple** of d.

Examples:

$$3|12 \,, \quad 12 \nmid 3 \,, \quad -7|35 \,.$$

(b) Problem Show that $0 \nmid a$ if $a \neq 0$. Also show, however, that according to our definitions, we do have $d|0$, for any integer d. Indeed, $0|0$.

(c) **Application 1 of $\lfloor\ \rfloor$:** If d and n are positive integers, how many multiples of d are there between 1 and n inclusive?

Solution: Each multiple of d looks like qd for various integers q. So what we must do is count all q's which make

$$1 \leq qd \leq n \,,$$

that is,

$$\frac{1}{d} \leq q \leq \frac{n}{d} \,.$$

But q is an integer, so we *really* have

$$\lceil \frac{1}{d} \rceil \leq q \leq \lfloor \frac{n}{d} \rfloor \,.$$

But $\lceil \frac{1}{d} \rceil = 1$, so we must count the positive integers from 1 to $\lfloor \frac{n}{d} \rfloor$ inclusive. We're done!

Answer: There are $\lfloor \frac{n}{d} \rfloor$ multiples.

For example, between 1 and $100,000$, there are

$$\lfloor \frac{100,000}{26} \rfloor = \lfloor 3846.15... \rfloor = 3846$$

multiples of 26.

(d) **Application 2 of $\lfloor\ \rfloor$: the Division Algorithm which underlies ordinary long division**.

For any integer a and any positive integer d, there are unique integers q (the **quotient**) and r (the **remainder**) such that

$$a = qd + r \quad , \quad 0 \leq r < d.$$

(a) Remark: We always use a positive divisor d in division. But with slight changes we could allow $d < 0$, too.

(b) Examples.

77	$= 25(3) + 2,$	so	$q = 25,$	$r = 2$
-77	$= (-26)(3) + 1,$	so	$q = -26,$	$r = 1$
75	$= 25(3) + 0,$	so	$q = 25,$	$r = 0.$

Indeed, $3|75$.

(c) Hint as to why the algorithm works: Let $q = \lfloor \frac{a}{d} \rfloor$, so $q \le \frac{a}{d} < q+1$.
Now let $r = a - qd$.
Just by the way we defined things, $a = qd + r$. There is more, however, to be proved in the next item.

(e) Problem To prove that division behaves as claimed, you must

(a) show that the remainder r, as defined above, actually does satisfy $0 \le r < d$;

(b) show that q, r are unique: no *other* integers will satisfy both $a = qd + r$ and $0 \le r < d$.

(f) Problem Show that the set of possible remainders after division by d is exactly

$$\{0, 1, 2, \ldots, d-1\} \,.$$

8.3 Another application of these ideas: modular arithmetic

(a) In modular arithmetic (sometimes called clock arithmetic in elementary school), we *fix* a positive integer d, called the **modulus**. For example, we take $d = 12$ for the usual clock.

In modular arithmetic, we may add, subtract and multiply any integers $x, y \in \mathbb{Z}$ as follows:

(a) calculate $x + y$ or $x - y$ or xy as ordinary integers;

(b) replace this preliminary result by its remainder (or **residue**) after division by d.

(c) we then get $x + y \pmod d$ or $x - y \pmod d$ or $xy \pmod d$, respectively.

(b) For example, take $d = 7$, as in weekly calculations. A complete set of **residues**, i.e. possible remainders, is $\{0, 1, 2, 3, 4, 5, 6\}$. So in modular arithmetic, every answer should be one of these residues.

Thus,

(a) $123 + 468 \equiv 3 \pmod 7$, since $591 = (84) \cdot 7 + 3$;

(b) $123 - 468 \equiv 5 \pmod 7$, since $-345 = (-50) \cdot 7 + 5$;

(c) $123 \cdot 468 \equiv 3 \pmod 7$, since $57564 = (8223) \cdot 7 + 3$.

(c) Modular division, however, is not so simple, although it does behave 'normally', when d happens to be a prime number.

Because modular arithmetic behaves rather differently from ordinary arithmetic, we use the symbol $\equiv$ to indicate modular equality. Thus $15 \equiv 3 \pmod{12}$, since both 15 and 3 have the same remainder, namely 3, when divided by 12.

For similar reasons, we write $100 \equiv 65 \pmod 7$.

Generally, for any modulus d and integers x, y we write

$$x \equiv y \pmod d$$

if x and y have the same remainder after division by d.

Thus $x \equiv y \pmod d$ does not mean that x and y have to be equal; rather they are *equivalent* in the sense of having an interesting property in common.

(d) Problem

(a) Show that the statement $x \equiv y \pmod d$ is the same thing as saying that $x - y$ is a multiple of d.

(b) Describe *all* integers x such that

$$5 - x \equiv 2 \pmod{7} .$$

Here are two more items, that we may or may not need in the course.

(e) **Primes:** A **prime number** p is any integer larger than 1 which has no proper divisors. (That is, its only proper divisors are $\pm 1, \pm p$.)

(f) Problem Find a text on number theory for the necessary background here.

(a) Use the sieve of Eratosthenes to determine by hand all primes less than 200.

(b) Find Euclid's proof that there are infinitely many prime numbers.

(c) Use Maple to determine the number of primes less than 1000, less than 100,000.

(d) What does the prime number theorem say about the approximate number of primes less than some large positive integer n?

(e) Prove the following theorem, which is due to Euclid, I think: Suppose p is a prime and $p|(ab)$. Then either $p|a$ or $p|b$ (or both).

(g) Suppose a, b are two integers, perhaps equal but not both 0. Then the **greatest common divisor** of a, b is the largest integer d dividing both a and b:

$$d|a \ , \quad d|b \ , \quad d \text{ largest.}$$

We write $d = \gcd(a, b)$.

(h) Problem: a few little exercises on $\gcd(a, b)$.

(a) Explain why we insist a, b are not both 0.

(b) If $d = \gcd(a, b)$,then $1 \leq d \leq \min(|a|, |b|)$.

(c) If $a = \pm b \neq 0$, then $\gcd(a, b) = |a|$.

(d) If $a|b$, then $\gcd(a, b) = |a|$.

(e) If $k|a$ and $k|b$, then for any integers x, y we have $k|(xa + yb)$.

(f) If $k|a$ and $k|b$, then $k|\gcd(a, b)$. (This is surprisingly tricky: we are saying that any common divisor of a and b must in fact divide the *greatest* such: it isn't obvious!)

8.4 More on Sets

(a) **Descriptions:** Sets are often described in an indirect, but nevertheless exact, manner. For example, think about

$$A = \{x : x \text{ is a positive divisor of } 777\}.$$

Thus $1 \in A$ but $2 \notin A$. Lots of work can be involved in explicitly describing all the elements of A.

Problem

(a) Describe all elements of A explicitly, something like this:

$$A = \{1, \ldots, 777\} .$$

(b) The number of elements in a set B is its **size** or **cardinality**, denoted $|B|$. What is $|A|$, for the set A described just above?

(c) Give an example of a set with infinitely many elements.

(b) **Subsets and Theorems:** Recall that A is a **subset** of B, written

$$A \subset B \qquad \text{(sometimes } A \subseteq B\text{)}$$

if every element of A is also an element of B. For example, if

$$A = \{x^2 : x \text{ is an integer}\} \text{ and } B = \{\text{non-negative integers}\},$$

then $A \subset B$ (why?). Notice, however, that B is not a subset of A, written

$$B \not\subset A,$$

since, for example, $5 \in B$ but $5 \notin A$.
Now in this example we can produce an explicit, though incomplete, description:

$$\begin{aligned} A &= \{0, 1, 4, 9, 16, 25, \ldots\} \\ B &= \{0, 1, 2, 3, 4, 5, \ldots\}. \end{aligned}$$

However, this is not really needed. The assertion that $A \subset B$ really amounts to a very simple fact from number theory:
Theorem: If x is any integer, then x^2 is a non-negative integer. In fact, any theorem of the sort

"If (statement 1), then (statement 2)"

really amounts to asserting $A \subset B$ for appropriate sets A, B.

(c) **An Example:** Look at these sets:

$$\begin{aligned} A &= \{\text{ prime numbers which leave remainder 1 when divided by 4}\} \\ B &= \{\text{ integers which are sums of two squares}\}. \end{aligned}$$

Thus $5 \in A$, $13 \in A$, $7 \notin A$, $25 \notin A$,

$$\begin{aligned} 5 \in B &\quad (\text{since } 5 = 1^2 + 2^2), \\ 25 \in B &\quad (\text{since } 25 = 3^2 + 4^2 = 0^2 + 5^2) \\ 7 \notin B &\quad (\text{Why?}). \end{aligned}$$

It is true, but rather hard to prove, that $A \subset B$.

(d) Problem

(a) What "if-then" type theorem lies behind the innocent looking expression $A \subset B$ in the previous example?

(b) Give the converse "if-then" type statement which corresponds to $B \subset A$. Is $B \subset A$? Is the converse statement a theorem (i.e. is the statement true)?

(c) Convince yourself that $p = 601$ is a prime number. Can it be written as a sum of two squares? If so, how?

(e) **Equality of Sets**. Two sets A, B are **equal**, written

$$A = B$$

if they have the same elements. Thus, to verify that two sets are equal we must show two things:

- every element of A is an element of B, so $A \subset B$; and
- every element of B is an element of A, so $B \subset A$.

(f) Now let's look at equality of sets in logical terms. Suppose

$$\begin{aligned} A &= \{x : \text{statement 1 is true}\} \\ B &= \{x : \text{statement 2 is true}\} \end{aligned}$$

Then $A = B$ corresponds to the
Theorem: Statement 1 if and only if statement 2 .
Why do we say this?

(a) "Statement 1 if statement 2" really means
"If statement 2, then statement 1",
i.e. $B \subset A$.

(b) "Statement 1 only if statement 2" really means
"Statement 1 forces statement 2", which really means
"If statement 1, then statement 2",
i.e. $A \subset B$.

(g) Problem Let

$$\begin{aligned} A &= \{\text{triangles whose sides } a, b, c \text{ satisfy } a^2 + b^2 = c^2\} \\ B &= \{\text{triangles with a right angle}\} \end{aligned}$$

(a) In fact, $A = B$. Write this as an "if and only if" type Theorem. (Don't prove anything!)

(b) Who usually gets credit for proving the theorem which corresponds to $B \subset A$?

(h) **That feeling of emptiness** ...
Let

$$A = \{2, 3, 4\} \text{ and } B = \{2, 4\}.$$

Thus $B \subset A$. However $B \notin A$ since $\{2, 4\}$ is **not** an individual member of the class. In essence, A and B have the same level of organization, so that B cannot belong to A.
Now let's drop elements from B:

$$C = \{4\}.$$

Again $\quad C \subset A : \quad \{4\} \subset \{2, 3, 4\}$
and $\quad C \notin A : \quad \{4\} \notin \{2, 3, 4\}$
Mind you, we still have $4 \in \{2, 3, 4\}$.
Finally, let's empty C:

$$E = \emptyset = \{\}.$$

Again $\quad \emptyset \subset A : \quad \{\} \subset \{2, 3, 4\}$
but $\quad \emptyset \notin A : \quad \{\} \notin \{2, 3, 4\}$.

(i) Problem Find the smallest set A such that $\{1\} \in A$ and $\{1\} \subset A$. What is $|A|$?

$* * * *$

(j) If you think about it, there's nothing special about the set $A = \{2, 3, 4\}$. We can empty any set of its contents and thus exhibit the empty set as a subset. Here is a formal version of this idea:

Theorem: If E is an empty set and A is any set, then

$$E \subset A.$$

Proof. The only way that $E \subset A$ could fail would be for E to have some element x which A does not:

$$x \in E \text{ and } x \notin A.$$

But E is empty: there is no such x. Thus $E \subset A$ (end of proof).

(k) It follows that if E_1 and E_2 are two empty sets, then

(a) letting E_1 play the role of E and E_2 the role of A we get $E_1 \subset E_2$.

(b) reversing roles, we get $E_2 \subset E_1$.

Hence $E_1 = E_2$. Thus any two empty sets are in fact equal. Since there is really only *one* empty set we are justified in creating a special symbol for it:

$$\emptyset = \underline{\text{the one and only}} \text{ empty set.}$$

Sermon: We shall seldom need to worry about such logical delicacies. There is, however, a remarkable outcome of all this: starting just with the empty set $\emptyset$ and using the symbols $\{\}$, $\in$ and $\subset$ in a creative way, we can actually **define** the number 0, then 1, then all integers, all reals, etc. That is

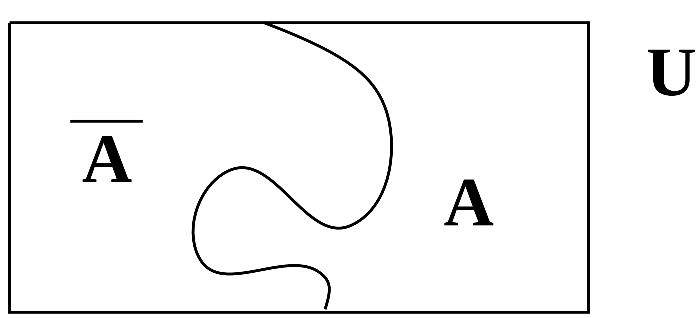
All mathematics can be created from nothing – sort of.

(l) **At the other end of Universe** ... The **universe** U is the set of all things we are interested in. Thus U is user-defined.

If we have agreed on a universe U, then every subset $A \subset U$ has a **complement**

$$\overline{A} = \{x \in U : x \notin A\}.$$

Diagrammatically we have



(m) **Altogether Now** ...
The **union** of two sets X and Y is the set $X \cup Y$ consisting of all elements in either X or Y (or both).
The **intersection** is the set $X \cap Y$ consisting of all elements in both X and Y ("simultaneously").
Both these definitions extend to three or more sets.
For example, let

$$\begin{aligned} X &= \{\text{positive multiples of 5 which are less than 43}\} \\ Y &= \{\text{positive multiples of 7 which are less than 43}\} \end{aligned}$$

Thus

$$\begin{aligned} X &= \{5, 10, 15, 20, 25, 30, 35, 40\} \\ Y &= \{7, 14, 21, 28, 35, 42\} \\ X \cap Y &= \{35\} \text{ (the lowest common multiple of 7 and 5 is 35)} \\ X \cup Y &= \{5, 7, 10, 14, 15, 20, 21, 25, 28, 30, 35, 40, 42\} \end{aligned}$$

Although 35 lies in both X and Y we need not write it twice in $X \cup Y$, since one indication is enough to tell us that $35 \in X \cup Y$.

(n) Problem Suppose

$$\begin{aligned} X &= \{\text{positive multiples of 48}\} \\ Y &= \{\text{positive multiples of 42}\}. \end{aligned}$$

(a) Is $X \cap Y$ finite?
(b) What is the smallest element of $X \cap Y$?
(c) What is the smallest element of $X \cup Y$?

(o) **Splitting the Pie**. Sometimes it's useful to cut, or **partition**, a set V into two or more pieces (which we call **classes**). Let's think about how we cut a pie V into two pieces X and Y:

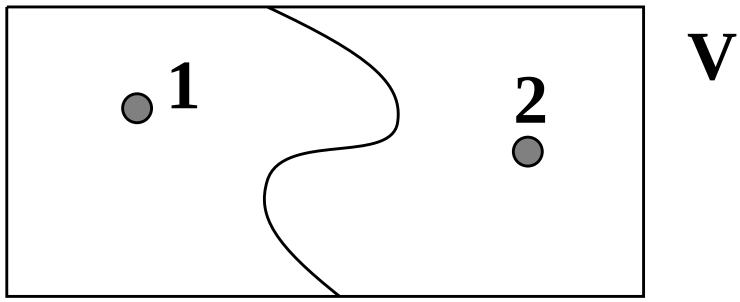
(a) $X \subset V$ and $Y \subset V$ (each piece is part of the whole pie).
(b) $X \neq \emptyset$, $Y \neq \emptyset$ (each piece has something in it).
(c) $X \cap Y = \emptyset$ (the pieces have nothing in common of course).
(d) $X \cup Y = V$ (the whole pie is used up by the pieces – there are no left-overs).

In short, a **partition** of a set V into two classes consists of a pair (X, Y) of non-empty, disjoint subsets X, Y whose union is V.

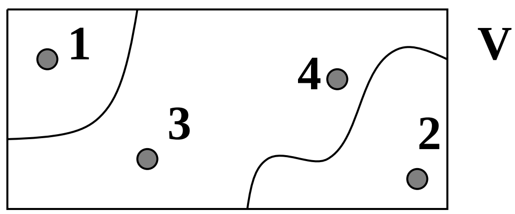
For example, $V = \{1, 2\}$ has only one partition, namely

$$(X = \{1\},\ \ Y = \{2\}).$$

Here is a diagram:



In a similar way we can define a partition into three or more classes: here is just one way for $V = \{1, 2, 3, 4\}$:



Partition = ({1}, {2}, {3,4})

(p) Problem

(a) How many different ways are there to partition $V = \{1, 2, 3\}$ into <u>two</u> classes?

(b) How many different ways are there to partition $V = \{1, 2, 3, 4\}$ into <u>two</u> classes? What about <u>three</u> classes? What about <u>four</u> classes?

9 References.

All these and many others are available in the library.

A. * G. Polya's "How to Solve It" is a highly recommended classic.

* H. Steinhaus' "Mathematical Snapshots" is one of several books which explore beautiful corners of mathematics in a simple yet challenging way.
* R. Honsberger's "Mathematical Gems" and "Mathematical Morsels"

B. The starred items are easier; most contain background material, so you don't have to be an expert.

1. Donald J. Newman, "A Problem Seminar", QA 43 N43.

*2. Loren C. Larson, "Problem Solving Through Problems", QA 43 L37.

3. "The William Lowell, Putman Mathematical Competition: Problems & Solutions 1938-1964".

*4. G. Polya - several other books - eg. "Mathematics & Plausible Reasoning".

5. M. Gardner - several books, plus any issue of "Scientific American" of the 1950's, 1960's, 1970's.

6. W. A. Wickelgren, "How to Solve Problems".

*7. The Contest Problem Book I, II, III, IV (American High School Math. Contests with Solutions). QA 43, S213, etc.

*8. International Mathematical Olympiads: QA 99 155. (The international version of (7)).

9. The Green Book, QA 43. H46.

C. Also several mathematics journals, available in the library, have monthly problem sections. Readers are invited to submit solutions, the best of which are published sometime later:

*(1) Mathematics Magazine

(2) Mathematical Gazette

*(3) Crux Mathematicorum (available in the Math/Stat Dept.)
(4) American Mathematical Monthly

(5) Mathematical Intelligencer

etc.

There is a huge international community of problem and puzzle enthusiasts. Why not join and get your name in print!