Addition of two sets of integers†

R. Balasubramanian* and Gyan Prakash

The Institute of Mathematical Sciences, CIT Campus, Taramani, Chennai 600 113, India

Let A be a subset of integers (or a subset of a finite abelian group); in this communication, we survey some results related to the properties of the set A from the information on cardinality of $2A$ or certain additive representation function associated to it.

Let , denote the set of integers and natural numbers, respectively. Given a finite set A, $|A|$ denotes the number of elements of A (also called the cardinality of A). Given A a subset of and $h \in$, we define

$$hA = \{b \in : b = a_1 + a_2 + \cdots + a_h, \text{ where } a_i \in A, \quad 1 \le i \le h\}.$$

For example, if $A = \{1, 2, 3, 4\}$, then

$$2A = \{2, 3, 4, 5, 6, 7, 8\} \text{ and}$$
$$3A = \{3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}.$$

If G is an abelian group, written additively and if $A \subset G$, $h \in$, we define hA in the same way.

A *direct problem* in additive number theory is one in which we try to determine the structure and the properties of the h-fold sumset hA, when the set A is known. On the other hand, an *inverse problem* is one in which we attempt to deduce the properties of the set A from the properties of the sumset hA.

Here, we will discuss some inverse problems. We will only consider the case when $h = 2$. Next, we will define for any infinite subset A of , certain 'additive representation functions' and discuss some problems where properties of A are determined by some unusual properties of such functions.

Let A be a finite subset of either the natural numbers or more generally of an abelian group $(G, +)$. Let $|A| = k$. Then, $|2A|$ can be as large as $k^2/2$. But suppose $|2A|$ is unusually small (say $|2A| < ck$, where c is a positive number), then can one deduce from this any information about the structure of A?

We discuss the case when A is a subset of and also the case when A is a subset of a finite abelian group. For further study of the problems discussed here, the reader may refer to an excellent book by Nathanson[1].

Let us consider the inverse problem for subsets of .

Theorem 1. Let A be a finite subset of natural numbers of cardinality k. Then $|2A| \ge 2k - 1$.

Proof: Say $A = \{a_1 < a_2 < \cdots < a_k\}$.

Then the elements $a_1 + a_1, a_1 + a_2, \cdots a_1 + a_k$, $a_2 + a_k$, $a_3 + a_k$ are distinct (being an increasing sequence) and are in $2A$, thus proving the theorem. □

Suppose A is an arithmetic progression of length k, i.e. $A = \{a_1, a_1 + d, \cdots, a_1 + (k-1)d\}$. Then $2A = \{2a_1, 2a_1 + d, 2a_1 + 2d, \cdots, 2a_1 + (2k-2)d\}$, i.e. $|2A| = 2k - 1$. This shows that result of the previous theorem is best possible.

The following result is the simplest inverse theorem in additive number theory.

Theorem 2. Let A be a finite subset of natural numbers of cardinality k. Then $|2A| = 2k - 1$ implies that A is an arithmetic progression.

Proof: Let $A = \{a_1 < a_2 < \cdots < a_k\}$. To prove that A is an arithmetic progression what we need to show is that for $2 \le i \le k - 1$ we have $a_i - a_{i-1} = a_{i+1} - a_i$, which is the equivalent of showing that $2a_i = a_{i-1} + a_{i+1}$. All the terms of the following sequence are distinct (being increasing) and belong to $2A$.

$$a_1 + a_1, a_1 + a_2, a_2 + a_2, a_2 + a_3, \cdots,$$
$$a_{i-1} + a_i, a_i + a_i, a_i + a_{i+1}, \cdots,$$
$$a_{k-1} + a_k, a_k + a_k. \qquad (1)$$

The length of this sequence is $2k - 1$. Then $|2A| = 2k - 1$ implies that any element of $2A$ belongs to the sequence given in eq. (1). This means that the only element of $2A$ which belongs to the interval $(a_{i-1} + a_i,\ a_i + a_{i+1})$ is $a_i + a_i$. But $a_{i-1} + a_{i+1} \in (a_{i-1} + a_i,\ a_i + a_{i+1}) \subset (2A)$, so $2a_i = a_{i-1} + a_{i+1}\ \forall\ 2 \le i \le k - 1$, which proves the theorem. □

Theorems 1 and 2 characterize those sets $A \subset$ having k elements and $|2A| < 2k$. Freiman proved the following:

Theorem 3. (Freiman): Let A be a subset of natural numbers and $|A| = k$. Suppose $|2A| = 2k - 1 + b \le 3k - 3$, then A is a subset of an arithmetic progression of length $k + b$.

For proof of the result see ref. 1.

A finite n-dimensional arithmetic progression is a set of the form

$$\{q_0 + x_1 q_1 + \cdots + x_n q_n : 0 \le x_i < l_i \text{ for } i = 1, \cdots, n, \text{ where } q_0, q_1, \cdots, q_n, l_1, l_2, \cdots, l_n \in \}.$$

In 1964, Freiman discovered a deep and beautiful fact about the structure of finite set of integers with small sumsets.

Theorem 4. (Freiman): Let $C \ge 2$. If A is a finite set of integers such that $|A| = k$ and $|2A| \le ck$, then A is a subset

†Dedicated to Prof. S. Ramaseshan on his 80th birthday.

*For correspondence. (e-mail: {balu,gyan}@imsc.res.in)

of an n-dimensional arithmetic progression Q, where $|Q| \leq c'k$, and n and c' are constants that depend only on c.

Nothing is known, however, about the structure of the finite set A, if, for example $|A| = k$ and

$$|2A| \leq k^{1+\delta}$$

for some $\delta > 0$, or even if

$$|2A| \leq ck \log k.$$

Nor is anything known about the structure of A, if for some $h \geq 3$,

$$|hA| \leq ck^{h-1},$$

or even $|hA| \leq ck^2$.

Example: Let A be a subset of , $|A| = k$. Then $\forall h \in$, prove that $|hA| \geq hk - (h-1)$.

Now we shall discuss the basic inverse problem when A is a subset of a finite abelian group G. In this case also we have results analogous to those of the previous section, where A was a subset of .

Definition: An arithmetic progression in an abelian group G is a set of the form $\{a + id : i = 0, 1, \cdots, k-1\}$. The group element d is called the *common difference* of the progression, and k is called the length of the progression. The order of the group element d in G *must* be at least k, which is to ensure that all elements of the progression are distinct.

We shall consider only a finite abelian group G. The first question we can ask is whether there is a suitable modification of Theorem 1 when A is a subset of the finite abelian group G. In this case, we cannot have $|2A| \geq 2|A| - 1$, as the case when $A = G$ itself provides a counter example. Also, as $2A \subseteq G$, so if $|A| > (|G|/2)$, then also we cannot have $|2A| \geq 2|A| - 1$.

Theorem 5. Let G be a finite abelian group. If A, $B \subset G$ such that $|A| + |B| > |G|$, then $A + B = G$.

Proof: Take any $g \in G$. Then consider the set $C = g - B = \{g - b: b \in B\}$. To prove $g \in A + B$, we observe that the sets A and C cannot be disjoint, because otherwise $|A \cup C| > |G|$. This gives the result. □

Even the modified statement, $|2A| \geq \min\{|G|, 2|A| - 1\}$ is not true in general; for example, when A is a nontrivial proper subgroup. But in the case when $G =$ $/p$, p is a prime number, we have the following theorem.

Theorem 6. Let p be a prime number and $A, B \subset$ $/p$. Then $|A + B| \geq \min\{p, |A| + |B| - 1\}$.

For the proof of the result see ref. 1.

The following theorem of Freiman–Vosper is analogous to Theorem.

Theorem 7. (Freiman–Vosper): Let p be a prime number and A be a non-empty subset of $/p$. If $|A| = k \leq (p/35)$ and $|2A| = 2k - 1 + b \leq 2.4k$, then A is a subset of an arithmetic progression of length $k + b$.

The proof uses two fundamental methods in additive number theory. The first is the estimation of exponential sums to construct a 'large' subset of a set $A \subseteq$ $/p$. The second is the use of arithmetic arguments to replace the set A of congruence classes with a set T of integers, such that there is a one-to-one correspondence between the elements of the subsets $2A$ and $2T$. The theorem is an easy corollary of the following proposition and Theorem 3.

Proposition 1. Let A be a set as in the statement of Theorem 7. Then, there exist $u \in$ $/p$ and $v \in ($ $/p$ $)^*$ satisfying the following:

Given $a \in A \; \exists \, t \in$, $0 \leq t \leq (p-1)/2$, such that $a = u + vt \pmod{p}$.

We will show how to deduce Theorem 7 from this proposition. For complete details of the proof of Theorem 7, we refer the reader to ref. 1.

Proof of Theorem 7: To prove Theorem 7, we observe the following:

(I) If $C, D \subset$ $/p$ such that $C = u_1 + v_1 D$, where $u_1 \in$ $/p$, $v_1 \in ($ $/p$ $)^*$, then C is a subset of an arithmetic progression of length l, if and only if D is so.

(II) Let C and D be the sets as above and p be a prime number not equal to 2. Then elements of C, $2C$ are in one-one correspondence with D and $2D$, respectively. So we have $|C| = |D|$ and $|2D| = |2C|$.

(III) Let $B \subset$ $/p$ of cardinality l, such that $b \in B$ implies that $b \equiv t \pmod{p}$ for some $t \in$, $0 \leq t \leq (p-1)/2$. Suppose further that $|2B| = 2l - 1 + m < 3l - 3$, then B is a subset of an arithmetic progression of length $l + m$.

To prove (III), we need Theorem 3. We define $T_B = \{t \in$: $0 \leq t \leq (p-1)/2$, $t \equiv b \pmod{(p)}$ for some $b \in B\} \subseteq$. Then to prove (III), it is sufficient to prove that T_B is a subset of an arithmetic progression of length $l + m$. The fact that $T_B \subset [0, (p-1)/2]$ implies that elements of $2B$ and $2T_B \subset$ are in one-one correspondence. Then, using Theorem 3 we get (III). It is straightforward to verify (I) and (II). Now from Proposition 1 we have $A = u + vB$, where $u \in$ $/p$, $v \in ($ $/p$ $)^*$, and B satisfies the hypothesis of (III). This gives the result. □

Ruzsa[2] has proved the following result which is analogous to Theorem 4.

Theorem 8. Let $r \geq 2$ be an integer and let G be an abelian group in which the order of every element is at most r. Let $A \subset G$ be a finite set, $|A| = n$. If $|A + A| \leq \alpha n$, then A is contained in a subgroup of G such that

$$|H| \leq cn,$$

where c depends only on r and α and is independent of n.

Now we will discuss some problems where properties of A are determined by some unusual properties of 'additive representation functions' associated to A.

For $A \subset$, $n \in$, the solutions of the equations

$$a + a' = n \quad a, a' \in A$$

$$a + a' = n \quad a, a' \in A, a \leq a'$$

$$a + a' = n \quad a, a' \in A, a < a'$$

are denoted by $r_1(A, n)$, $r_2(A, n)$, $r_3(A, n)$ respectively and are called additive representation function associated with A. In case there is no ambiguity, $r_1(A, n)$, $r_2(A, n)$, $r_3(A, n)$ are denoted by $r_1(n)$, $r_2(n)$, $r_3(n)$. For example when $A =$, then the reader can verify that $r_1(6) = 5$, $r_2(6) = 3$, and $r_3(6) = 2$. Also, when $A = \{1, 3, 5, 7, \cdots\}$, i.e. the set of all odd natural numbers, then $r_i(2k - 1) = 0$ $\forall 1 \leq i \leq 3, k \in$, and $r_1(6) = 3, r_2(6) = 2$ and $r_3(6) = 1$.

Now we will discuss some problems where properties of A are determined by some properties of $r_i(n)$ (i may be 1, 2 or 3). For further study of such problems, the readers may refer to an excellent book by Halberstam and Roth[3] and a survey article on this topic by Sárközy and Sós[4].

Consider the case when $r_i(n)$ is monotonic. As $r_i(n)$ are always non-negative integers, so if $r_i(n)$ is monotonically decreasing, then it is constant from a certain point on. Thus it is enough to consider the case when $r_i(n)$ is non-decreasing. Here, monotonic means monotonically non-decreasing.

In 1941, Erdõs and Turán proved that for an infinite set $A \subset$, the representation function $r_1(n)$ cannot be a constant from a certain point on. Dirac and Newman proved that the same holds with $r_2(n)$ in place of $r_1(n)$.

Theorem 9. (Dirac and Newman; ref. 4). For an infinite set $A \subset$, the representation function $r_2(n)$ cannot be a constant from a certain point on.

Proof: Let $f(x) = \sum_{a \in A} x^a$ (for x real, $|x| < 1$).

Then the reader can easily verify that

$$\frac{1}{2}(f^2(x) + f(x^2)) = \sum_{n=0}^{+\infty} r_2(n) x^n.$$

If $r_2(n) = k$ for $n > m$, then

$$\frac{1}{2}(f^2(x) + f(x^2)) = \sum_{n=0}^{+\infty} r_2(n) x^n = P_m(x) + k \frac{x^{m+1}}{1 - x},$$

where $P_m(x)$ is a polynomial of degree $\leq m$. If $x \to -1$ from the right, then the right-hand-side has a finite limit, while the left-hand-side tends to $+\infty$. This contradiction proves the theorem.

□

Erdõs *et al.*[5] proved the following theorem. The first author of this article[6] has provided a different proof of their result and also improved it.

Theorem 10. (Refs 5 and 6) Let A be a subset of . Then we have the following:

(I) If for some $n_0 \in$, $r_1(n + 1) \geq r_1(n)$ $\forall n \geq n_0$, then either A is a finite set or A^c contains all but finitely many natural numbers.

(Here A^c denotes the set of all natural numbers $\notin A$.)

(II) If for some $n_0 \in$, $r_2(n + 1) \geq r_2(n)$ $\forall n \geq n_0$, then for any $N \in$, the number of natural numbers $\in A^c$ and less than N is at most c (ln N), where c is a positive absolute constant.

(III) It is possible that A has infinitely many elements and for any $N \in$, the number of natural numbers $\in A^c$ and less than N is at least $c\, N^{1/3}$, where c is a positive absolute constant and also for some $n_0 \in$, $r_3(n + 1) \geq r_3(n)$ $\forall n \geq n_0$.

Remark 1: One of the key steps in the proof of Theorem 10 (I) is an observation by Erdõs *et al.*[5] on $r_1(n)$. Since in $r_1(n)$, the pairs (a_i, a_j) and (a_j, a_i) are considered distinct, it is clear that $r_1(n)$ is an even function, except when $n/2$ is an integer and $(n/2) \in A$.

Consequently, if we define

$$f(n) = 0 \text{ if } \frac{n}{2} \in A \text{ and } f(n) = 1 \text{ if } \frac{n}{2} \notin A,$$

then $r(n) \equiv f(n) \pmod 2$.

Then $r(n + 1) - r(n) = f(n + 1) - f(n) \pmod 2$.

Now recall the assumption of Theorem 10 (I) is that $r(n + 1) - r(n) \geq 0$ for all large n. If $f(n + 1) - f(n)$ is odd, then we immediately strengthen the given inequality.

Thus, if we define $\delta(n) = \begin{cases} 1 & \text{if either } \frac{n}{2} \text{ or } \frac{n+1}{2} \in A \\ 0 & \text{else,} \end{cases}$

we get $r(n + 1) - r(n) \geq \delta(n)$.

This strengthening enabled the authors to make strong conclusions in Theorem 10 (I), and since no such streng-

thening based on parity is known, it seems difficult to prove strong results regarding $r_2(n)$.

Now can we possibly have a set A with $r_1(n) = c$ for all large n, and for some $c > 0$? If such a set exists, then Theorem 10 (I) applies and we would have either A as finite or A^c as finite. But if A is finite, then $c = 0$, and if A^c is finite, then $r(n) \to \infty$. We thus conclude that such a set A does not exist. Now Erdõs and Fuchs proved that it is not even possible to have a set A, such that the mean value of $r(n)$ over $[1, N]$ is very close to c.

Theorem 11. (Erdõs and Fuchs; ref. 3). If A is an infinite subset of , then given any $c > 0$ we have

$$\limsup_{N\to\infty}\left\{\frac{(\sum_{n\le N} r(n)) - cN}{N^{1/4}(\log N)^{-\frac{1}{2}}}\right\} > 0.$$

One important problem in number theory is the circle problem, i.e. the estimate of the number of lattice points in the circle $x^2 + y^2 \le N$. Writing

$$\Delta(N) = |\{(x, y): x, y \in \ , x^2 + y^2 \le N\}| - \pi N,$$

the problem is to estimate $\Delta(N)$. If we apply Theorem 11, when $A = \{1^2, 2^2, 3^2, \cdots\}$, i.e. A is the set of squares, then we have

$$\limsup_{N\to\infty}\left\{\frac{\Delta(N)}{N^{1/4}(\log N)^{-\frac{1}{2}}}\right\} > 0.$$

This special case is the classical theorem of Hardy and Landau. (In this special case, as well in the general case, it is possible to improve the power of (log N). We do not go into these minor details here, even though these are the bread and butter for number theorists.)

Consider the case when $r_i(n)$ is small. A set A is called a sidon set if $r_2(n) \le 1$ for all n. (Recall $r_2(n)$ is the number of representations of $n = a_i + a_j$, with $a_i \le a_j$.) Let $A \subseteq [1, N]$ be a sidon set. How large can $|A|$ be?

Clearly the map T: $\{(a_i, a_j)$: $a_i < a_j$; $a_i, a_j \in A\} \to [1, N]$ defined by $T(a_i, a_j) = a_j - a_i$ is (1–1). Thus, $|\{a_i, a_j)$: $a_i < a_j$; $a_i, a_j \in A\} \le N$.

This gives $\frac{|A|^2 - |A|}{2} \le N$, yielding $|A| < \sqrt{2N} + 1$.

By an ingenious argument, Erdõs and Turán (see ref. 3) proved that it can be improved to $|A| \le (1 + \varepsilon)\sqrt{N}$. It was proved by Bose and Chowla (see ref. 3) that this result is the best possible. (We warn the readers that we have ignored the lower order terms in these statements). Bose and Chowla constructed a set $A \subset [1, N]$, such that A is a sidon set and $|A| \ge \sqrt{N}$.

The construction of A by Bose and Chowla is as follows. For any prime p, consider $_{p^2}$ to denote the finite field with p^2 elements, and let α be a generator of the cyclic group $^*_{p^2}$. Then for all $c \in \ _p$, we have unique $a(c)$ such that $\alpha + c = \alpha^{a(c)}$ and $1 \le a(c) \le p^2 - 1$. Then clearly, $A = \{a(c)$: $c \in \ _p\} \subset [1, p^2 - 1]$ is a sidon set having p elements.

When $r_i(n) \ge 1$, we can ask the following question: Suppose A is an infinite $\subset$ such that $r_1(n) \ge 1$ for all $n \ge n_0$. Then is it possible that A is such that $r_1(n)$ is bounded for all n?

Erdõs and Turán conjecture that it is not possible. In this connection, Erdõs (see ref. 3) has proved by probabilistic arguments that there exists a set A such that $r_1(n) \ge 1$ for all $n \ge n_0$ and for some $c > 0$, $r_1(n)$ is less than c ln n for all n. (However no explicit construction is known.)

But if we want the set A to satisfy that mean value of $r_1(n)$ is bounded, then Ruzsa proved that it is possible.

Theorem 12. (Ref. 7): There is an infinite set $A \subset$ such that $r_1(n) \ge 1$ for all $n \ge n_0$, and there exists $c > 0$ such that

$$\frac{1}{N}\left(\sum_{1}^{N} r_1^2(n)\right) < c \forall N \in \ .$$

Consider the parity of $r_2(n)$. If A is an infinite subset of $\cup \{0\}$, then we set

$$A(x) = \{a \le x: a \in A\}.$$

Nicolas, Ruzsa and Sárközy asked the following question:

Let A be an infinite subset of $\cup \{0\}$ such that for some $n_0 \in$, $r_2(n)$ is even for all $n \ge n_0$. Then what can we say about $|A(x)|$ for sufficiently large x? How small or large can it be?

Practically nothing is known about this question. Fixing an $i \in \{0, 1\}$, it is easy to construct an infinite set $A \subset \ \cup \{0\}$ such that for some $n_0 \in$, we have $r_2(n) \equiv i \pmod 2$ for all $n \ge n_0$ using greedy algorithm.

Algorithm: We construct a set $A \subset \ \cup \{0\}$ recursively by the following algorithm, such that $r_2(n) \equiv i \pmod 2$ for all $n \ge m$, where $m > 3$ is a fixed natural number.

(I) Take any $B \subset \{0, 1, 2, \ldots, m - 3\}$, such that $0 \in B$.
(II) Assume that $A(l) = A \cap \{0, 1, 2, \ldots, l\}$ has been defined so that $r(A(l), n) \equiv i \pmod 2$ for $m - 2 \le n \le l$. Then,

$l + 1 \in A$ if and only if $r(A(l), l + 1) \equiv i - 1 \pmod 2$.

Consider the case when $r_2(n)$ is not equal to 1. Since the question regarding $r(n)$ being even for all $n \geq n_0$ seems difficult, let us ask (a hopefully simpler) question.

If A is a infinite subset of such that $r_2(n)$ is different from 1 for all $n \geq n_0$, how small can A be?

Let us start with an example.

Let $A = \{2^k + 2^l : k, l \in \cup \{0\}\}$, then $r_2(n)$ is different from 1 for all $n \geq 10$ and $|A(x)|$ is around $\frac{1}{2}(\ln x)^2$.

Nicolas *et al.*[8] proved the following theorem.

Theorem 13. If A is an infinite subset of such that $r(A, n) \neq 1$ for all sufficiently large natural numbers n, then

$$\limsup |A(x)| \left(\frac{\ln \ln x}{\ln x} \right)^{3/2} \geq \frac{1}{20}.$$

The authors of this article have proved the following result.

Theorem 14. (Ref. 9) There exists an absolute constant $c > 0$ with the following property: for any infinite subset A of such that $r(A, n) \neq 1$ for all sufficiently large natural numbers n,

$$|A(x)| \geq c \left(\frac{\ln x}{\ln \ln x} \right)^2 \text{ for all } x \text{ sufficiently large.}$$

This shows that the example which we discussed here is essentially best possible.

1. Nathanson, Melvyn, B., *Additive Number Theory, Inverse Problems and the Geometry of Sumsets*, Springer Verlag, 1991.
2. Ruzsa, I., An analog of Freiman's theorem in groups. *Asterisque*, 1999, **258**, 323–326.
3. Halberstam, H. and Roth, K. F., *Sequence*, Oxford University Press, 1996, vol. 1.
4. Sárközy, A. and Sós, V. T., On additive representation functions. In *The Mathematics of Paul Erdõs* (eds Nešetøil, J. and Graham, R. L.), Springer Verlag, 1991, vol. 1, pp. 129–150.
5. Erdõs, P., Sárközy, A. and Sós, V. T., Problems and results on additive properties of general sequences, III. *Stud. Sci., Math. Hung.*, 1987, **22**, 53–63.
6. Balasubramanian, R., A note on a result of Erdos, Sárközy and Sós. *Acta Arith.*, 1987, **49**, 45–53.
7. Ruzsa, I., A just basis. *Monatsh. Math.*, 1990, **109**, 145–151.
8. Nicolas, J. L., Ruzsa, I. Z. and Sárközy, A., On the parity of additive representation functions. *J. Number Theory*, 1998, **73**, 292–317.
9. Balasubramanian, R. and Gyan Prakash, On an additive representation function. *J. Number Theory* (accepted).

Received 29 September 2003

Fast and efficient algorithms for solving ordinary differential equations through computer algebra system

Pratibha

312/9, Mohit Nagar, Dehradun 248 006, India

Ordinary differential equations (ODE) occur in several branches of science and technology. One example may be study of particle interaction in electrorheological (ER) fluids. These are fluids whose properties change when they are exposed to an electric field. These fluids have important applications in many fields, automotive industries in particular. Calculations of interactions between particles suspended in fluid are carried out through the solution of ODE with regular singular point. Series solutions to such problems provide highly accurate results if a large number of terms in the series expansion are included. Based on this, several routines, to be used as a package in Computer Algebra System Maple®, are developed to solve the linear homogeneous ordinary differential equations with a regular singular point. These fast and efficient algorithms show significant improvements over existing routines in terms of memory and computational time requirements. The present algorithms provide the correct answer for many differential equations much more efficiently. Using these tools, a large number of terms in the series expansions can be included to get highly accurate solutions of ordinary differential equations.

COMPUTER Algebra Systems (CAS) are simply the programs which enable one to manipulate mathematical expressions symbolically. One of the biggest attractions of CAS is their ability to manipulate long expressions. For most computer literates, the word *computing* means number crunching or numerical calculations. Manipulation of complex mathematical expressions is considered a daunting task for computers. Before computers appeared on the scene, a calculation usually consisted of a mixture of numerical calculation and calculation by mathematical formulas or algebraic calculation. All the numerical calculations were preceded by a manipulation of algebraic formulas, if the work was to be within the bounds of what is humanly possible. In the 19th century, several large calculations have a substantial number of formula manipulations. Among the famous calculations was Le Verrier's calculation of the orbit of Neptune, which started from the disturbances of the orbit of Uranus, and led to the discovery of Neptune. The most impressive and probably the largest calculation with pencil and paper is by the French astronomer Charles Delaunay[1]. He took 10 years to calculate the orbit of the moon as a function of

e-mail: pratibhag@rediffmail.com