ARITHMETIC PROGRESSIONS IN SPARSE SETS

by

Mokhtar Taher Zobi

B.Sc., University of El-Fateh, 1979

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

in the Department

of

Mathematics and Statistics

SIMON FRASER UNIVERSITY

March 1986

APPROVAL

Name: Mokhtar Taher Zobi

Degree: Master of Science

Title of Thesis: Arithmetic Progressions in Sparse Sets

Examining Committee:

Chairman: Professor C. Villegas

Dr. A.R. Freedman
Senior Supervisor

Dr. J.J. Sember

Dr. C. Godsil

Dr. N.R. Reilly
External Examiner

Date approved: March 13, 1986

PARTIAL COPYRIGHT LICENSE

I hereby grant to Simon Fraser University the right to lend my thesis, project or extended essay (the title of which is shown below) to users of the Simon Fraser University Library, and to make partial or single copies only for such users or in response to a request from the library of any other university, or other educational institution, on its own behalf or for one of its users. I further agree that permission for multiple copying of this work for scholarly purposes may be granted by me or the Dean of Graduate Studies. It is understood that copying or publication of this work for financial gain shall not be allowed without my written permission.

Title of Thesis/Project/Extended Essay

ARITHMETIC PROGRESSIONS IN SPARSE SETS

Author: _____
(signature)

MOKHTAR TAHER ZOBI
(name)

MAY 15, 1986
(date)

ABSTRACT

We investigate arithmetic progressions in sparse sets. We further develop the theory of arithmetic progressions in M-lacunary sequences. In particular, there is a finite constant K_N, where $N \geq 3$, such that if A is a finite M-lacunary sequence and the sum of the reciprocals of the elements of A is greater than or equal to K_N, then A contains N consecutive terms in arithmetic progression. An investigation of arithmetic progressions in geometric progressions $\{f(n)\} = \{c^n\}$, where $c > 1$ is a real number and n is a non-negative integer is made. The topological structure of the set of all such c, where $\{c^n\}$ contains a 3-term arithmetic progression is discussed. Arithmetic progressions in quadratics $\{f(n)\} = \{\alpha n^2 + \beta n + \gamma\}$, where $\alpha > 0$ are also studied. In particular, necessary and sufficient conditions for $\{(an + b)^2\}$ to contain a three term arithmetic progression are given for most cases of a and b, where $a > b \geq 0$ and $(a,b) = 1$. Some unsolved problems are mentioned.

DEDICATION

to my parents

ACKNOWLEDGEMENT

It is a pleasure for me to record my gratitude to my Senior Supervisor, Dr. A.R. Freedman, for his generous advice and encouragement during the preparation of this thesis. I would like to thank him for his collaboration to obtain the main results of this thesis.

I would also like to thank Mrs. Sylvia Holmes for her excellent typing of this thesis.

TABLE OF CONTENTS

INTRODUCTION

The purpose of this thesis is to examine arithmetic progressions in sparse sets, that is, in sets which contain relatively few elements in terms of density.

In Chapter 1, we discuss arithmetic progressions in M-lacunary sequences. Brown and Freedman [1] have shown that, if A is an M-lacunary sequence and the sum of the reciprocals of the elements of A diverges, then A contains arbitrary long consecutive arithmetic progressions. We show that there is a finite constant K_N, where $N \geq 3$, such that if A is a finite M-lacunary sequence and the sum of the reciprocals of the elements of A is greater than or equal to K_N, then A contains N consecutive terms in arithmetic progression. We also find the optimal K_N for all $N \geq 3$. We show that, we can never force arbitrary long consecutive arithmetic progressions in an M-lacunary sequence A just by requiring the sum of the reciprocals of $a \in A$ to be large, but finite.

In Chapter 2, we investigate arithmetic progressions in geometric progressions $\{f(n)\} = \{c^n\}$, where C is a real number greater than 1 and n is a non-negative integer. Theorem 2.2 shows that, $\{c^n\}$ contains 3-term arithmetic progression if and only if c is a root of a polynomial equation

$$x^a - 2x^b + 1 = 0 ,$$

where a and b are positive integers such that $b < a < 2b$. We are led to an investigation of the topological structure of the set, S,

of all such c, where $c > 1$ and $\{c^n\}$ contains a 3-term arithmetic progression. In Theorem 2.6 we show that, the set of all cluster points of S is $T = \{\ell: \ell = 1 \text{ or } \ell = 2^{1/t} \text{ for some integer } t \geq 1\}$.

In Chapter 3, we analyze arithmetic progressions in quadratics $\{f(n)\} = \{\alpha n^2 + \beta n + \gamma\}$, where $\alpha > 0$. We show that $\{f(n)\}$ contains arithmetic progressions only if β/α is a rational. The problem then reduces to the essentially number theoretic problem of finding arithmetic progressions among sets of sequences $\{(an + b)^2\}$, where integers a and b satisfy $a > b \geq 0$, $(a,b) = 1$. Let

$$T = \{(a,b): \text{ } a \text{ and } b \text{ are integers, } a > b \geq 0, (a,b) = 1$$

and $\{(an + b)^2\}$ contains a primitive 3-term arithmetic progression$\}$. (Here "primitive" means that the three terms of the arithmetic progression are relatively prime.) Theorem 3.16 shows, when a is odd, that $(a,b) \in T$ if and only if b, $\frac{b}{2}$ or $\frac{b+a}{2}$ is a quadratic residue mod a.

For the case when a is even, we show that, if $a = 2^n$, then $(a,b) \in T$ if and only if b is a quadratic residue mod a. Other cases when a is even are discussed.

CHAPTER 1

CONSECUTIVE ARITHMETIC PROGRESSIONS IN M-LACUNARY SEQUENCES

First let us start this Chapter with the following definitions:

Definition 1.1. An increasing sequence $a_1 < a_2 < a_3 < \dots$ of natural numbers is called lacunary if $d_n = a_{n+1} - a_n \to \infty$ as $n \to \infty$, and called M-lacunary if, furthermore, $d_n \leq d_{n+1}$ for all n.

Definition 1.2. We define a finite increasing sequence, $a_1 < a_2 < \dots < a_k$ of natural numbers to be a finite M-lacunary sequence if $d_n \leq d_{n+1}$ for $n = 1,2,\dots,k-2$, where $d_n = a_{n+1} - a_n$.

Brown and Freedman [1] have shown that, if A is an M-lacunary sequence and $\sum_{a\in A} \frac{1}{a} = \infty$, then A contains arbitrarily long consecutive arithmetic progressions.

We ask whether or not there is a finite constant K_N, where $N \geq 3$, such that if A is a finite M-lacunary sequence and $\sum_{a\in A} \frac{1}{a} \geq K_N$. Then A has N consecutive terms in arithmetic progression.

We will show that K_N exists and find its smallest value exactly for each N. To do this we define a sequence $B_N = (b_i)_{i=1}^{\infty}$ as follows:

First let us agree to use $\underline{i}^N = (i,i,i,\dots,i)$ where there are N-terms as a notation. We define the difference sequence (d_n) of the sequence B_N, where $N \geq 3$, to be

$$(d_n) = (\underline{1}^{N-2},\underline{2}^{N-2},\underline{3}^{N-2},\dots) .$$

Let $b_1 = 1$ and $b_n = 1 + d_1 + d_2 + \ldots + d_{n-1}$, $n \geq 2$. Then

$$B_N = (1,2,3,\ldots,N-1,N+1,N+3,\ldots,N-1+2(N-2) = 3N-5,3N-2,$$
$$3N+1,\ldots,3N-5+3(N-2) = 6N-11,6N-7,6N-3,6N+1,\ldots).$$

It is clear that B_N is an M-lacunary sequence, and B_N does not contain N consecutive terms in arithmetic progression since (d_n) does not have $N-1$ consecutive equal terms.

Theorem 1.3. B_N has convergent sum of reciprocals.

Proof. From the definition of the sequence B_N, we can see that

$$b_1 = 1$$

$$b_2 = b_1 + d_1 = b_1 + 1 > 1$$

$$b_{2+(N-2)} \geq b_1 + d_1 + d_{1+(N-2)} = b_1 + 1 + 2 > 1 + 2$$

$$b_{2+2(N-2)} \geq b_1 + d_1 + d_{1+(N-2)} + d_{1+2(N-2)} = b_1 + 1 + 2 + 3 > 1 + 2 + 3$$

$$\ldots$$

$$b_{2+k(N-2)} \geq b_1 + d_1 + d_{1+(N-2)} + d_{1+2(N-2)} + \ldots + d_{1+k(N-2)}$$

$$= b_1 + 1 + 2 + 3 + \ldots + (k+1)$$

$$> 1 + 2 + 3 + \ldots + (k+1)$$

$$= \frac{(k+1)(k+2)}{2}$$

and so on. It follows that

$$\sum_{i=1}^{\infty} \frac{1}{b_i} = 1 + \sum_{i=2}^{\infty} \frac{1}{b_i}$$

$$= 1 + \sum_{k=0}^{\infty} \Big(\sum_{i=k(N-2)}^{(k+1)(N-2)-1} \frac{1}{b_{2+i}} \Big)$$

$$\leq 1 + (N-2) \sum_{k=0}^{\infty} \frac{1}{b_{2+k(N-2)}}$$

$$< 1 + (N-2) \sum_{k=0}^{\infty} \frac{2}{(k+1)(k+2)}$$

$$< 1 + 2(N-2) \sum_{k=0}^{\infty} \frac{1}{(k+1)^2} < \infty .$$

Thus the theorem is proved.

Let $\sum_{b \in B_N} \frac{1}{b} = K_N$.

We calculated some K_N by computer. For $N = 3,4,5$, we found that $K_3 \cong 2.3734$, $K_4 \cong 2.8745$, and $K_5 \cong 3.204$.

Because $K_N > \sum_{i=1}^{N-1} \frac{1}{i} \to \infty$ as $N \to \infty$, we get $K_N \to \infty$ as $N \to \infty$.

Now we have the following important theorem.

Theorem 1.4. Let A be a finite M-lacunary sequence. If $\sum_{a \in A} \frac{1}{a} \geq K_N$, then A contains N consecutive terms in arithmetic progression.

Before we give the proof of this theorem we need the following lemma.

Lemma 1.5. Let $(d_n) = (\underline{1}^{N-2}, \underline{2}^{N-2}, \underline{3}^{N-2}, \ldots)$, $N \geq 3$, and let (a_n) be an M-lacunary sequence (finite or infinite), with $t_n = a_{n+1} - a_n$, such that $t_i \geq d_i$ for all i, then $a_i \geq b_i$ for all i where b_i is the i-th term in B_N defined above.

Proof of Lemma 1.5. By induction, first $a_1 \geq 1 = b_1$. Assume it is true for j (i.e., $a_j \geq b_j$). Then

$$a_{j+1} = a_j + t_j \geq b_j + t_j \geq b_j + d_j = b_{j+1} .$$

Therefore it is true for $j + 1$, and hence $a_i \geq b_i$ for all i.

Now we are going to prove the Theorem 1.4. Let $A = (a_1, a_2, \ldots, a_k)$, let $t_i = a_{i+1} - a_i$, $i = 1, \ldots, k-1$. Assume A does not have N consecutive terms in arithmetic progression, it follows that

$$a_{i+N-1} - a_{i+N-2} > a_{i+1} - a_i , \quad i = 1,2,\ldots,k-N+1 ,$$

(i.e., $t_{i+N-2} > t_i$, $i = 1,2,\ldots,k-N+1$.)
Let $(d_n) = (\underline{1}^{N-2}, \underline{2}^{N-2}, \underline{3}^{N-2}, \ldots)$.
We want to show that $t_i \geq d_i$ for all $i = 1,2,\ldots,k-1$. It is clear that $t_j \geq 1 = d_j$, $j = 1,2,\ldots,N-2$. Let $i > N-2$ and assume $t_j \geq d_j$ for $j = 1,2,\ldots,i-1$. Then

$$t_i = t_{[i-(N-2)]+(N-2)} \geq t_{i-(N-2)} + 1 \geq d_{i-(N-2)} + 1$$

$$= d_i - 1 + 1 = d_i .$$

Therefore $t_i \geq d_i$ for $i = 1,2,\ldots,k-1$. Then by Lemma 1.5 it follows that

$$a_i \geq b_i \quad \text{for} \quad i = 1,2,\ldots,k \ .$$

Hence $\sum_{a\in A} \frac{1}{a} \leq \sum_{i=1}^{k} \frac{1}{b_i} < \sum_{b\in B_N} \frac{1}{b} = K_N$ which is a contradiction.

Thus $a_{i+N-1} - a_{i+N-2} = a_{i+1} - a_i$ for some i and $(a_i, a_{i+1}, \ldots, a_{i+N-1})$ are N consecutive terms in arithmetic progression.

Corollary 1.6. If $A = (a_i)$ is an infinite M-lacunary sequence, and $\sum_{a\in A} \frac{1}{a} > K_N$, then A has a consecutive N-term arithmetic progression.

Here is an example of a subset A of natural numbers such that A does not contain any 3-term arithmetic progression at all (not necessarily consecutive) and where one gets $\sum_{a\in A} \frac{1}{a} > K_3$.

Let $A = (1,2,4,5,10,11,13,14,28,29,31,32,\ldots)$. Then $\sum_{a\in A} \frac{1}{a} \cong 2.54 > K_3 \cong 2.3734$, but A does not contain a 3-term arithmetic progression. Hence the bound K_3 works only for M-lacunary sequences.

Remark 1.7. The bound K_N is optimal in the following sense.

For all $\varepsilon > 0$, there exists a finite M-lacunary sequence A such that $\sum_{a\in A} \frac{1}{a} > K_N - \varepsilon$ and A does not have N consecutive terms in arithmetic progression. This follows from the fact that $\sum_{b\in B_N} \frac{1}{b} = K_N$ implies that there exists n such that $\sum_{i=1}^{n} \frac{1}{b_i} > K_N - \varepsilon$. So if we take $a_i = b_i$, $i = 1,2,\ldots,n$, then A is a finite M-lacunary

sequence, $\sum_{a\in A} \frac{1}{a} > K_N - \varepsilon$ and A does not have N consecutive terms in arithmetic progression.

We can never force arbitrarily long consecutive arithmetic progressions in an M-lacunary sequence A just by requiring $\sum_{a\in A} \frac{1}{a}$ to be large, but finite. This is shown in the next theorem.

Theorem 1.8. For all $0 < T < \infty$, there exists an M-lacunary sequence A such that $\sum_{a\in A} \frac{1}{a} > T$, but A does not have arbitrary long consecutive arithmetic progressions.

Proof. Let $0 < T < \infty$ be given. We know that $\sum_{i=1}^{\infty} \frac{1}{i} = \infty$, it follows that there exists n such that $\sum_{i=1}^{n} \frac{1}{i} > T$. Let $A = (1,2,3,\ldots,n,n^2,n^3,\ldots)$. Then A is an M-lacunary sequence and $\sum_{a\in A} \frac{1}{a} > T$. But, since $n^{j+2} - n^{j+1} > n^{j+1} - n^j$ for all j, $n > 1$, A does not have arbitrary long consecutive arithmetic progressions.

However, Brown and Freedman [1] have shown that if A is an M-lacunary sequence and $\sum_{a\in A} \frac{1}{a} = \infty$, then A has arbitrary long consecutive arithmetic progressions.

Erdös' famous conjecture states that if A is a subset of natural numbers and $\sum_{a\in A} \frac{1}{a} = \infty$, then A contains arbitrary long arithmetic progressions. The proof (or disproof) of this is, at present, out of sight. In fact, it has not even been proved that $\sum_{a\in A} \frac{1}{a} = \infty$ implies that A has a 3-term arithmetic progression.

CHAPTER 2

ARITHMETIC PROGRESSIONS IN GEOMETRIC PROGRESSIONS

In this Chapter, we want to study three term arithmetic progressions in the set of values of an exponential function $\{f(n)\} = \{c^n\}$, where c is a real number greater than 1 and n is a non-negative integer.

Lemma 2.1. Let $c \geq 2$. Then $\{f(n)\} = \{c^n\}$ has no three terms in arithmetic progression.

Proof. Let $c \geq 2$ be fixed. Suppose $\{c^n\}$ has a three term arithmetic progression. It follows that there exist non-negative integers $n_1 < n_2 < n_3$ such that

$$c^{n_3} - c^{n_2} = c^{n_2} - c^{n_1},$$

or

$$c^{n_3-n_1} - 2c^{n_2-n_1} + 1 = 0 .$$

Let $a = n_3-n_1$ and $b = n_3-n_1$. Then

$$c^a - 2c^b + 1 = 0 , \tag{1}$$

where a and b are positive integers and $b < a$. Now, since $a \geq b+1$ and $c \geq 2$. Then

$$c^a - 2c^b \geq 0 ,$$

and so

$$c^a - 2c^b + 1 > 0 .$$

This is a contradiction. Hence $\{c^n\}$ has no three terms in arithmetic progression.

Now, we state and prove the following important theorem which shows a necessary and sufficient condition for $\{f(n)\}$ to have three terms in arithmetic progression.

Theorem 2.2. Let $c > 1$. Then $\{f(n)\} = \{c^n\}$ has three terms in arithmetic progression if and only if c is a root of a polynomial equation

$$g(x) = x^a - 2x^b + 1 = 0$$

where a and b are positive integers and $b < a < 2b$.

Proof. Suppose $\{c^n\}$ has a three term arithmetic progression. By virtue of Lemma 2.1, $\{c^n\}$ has no three terms in arithmetic progression for $c \geq 2$. It follows that we can assume c satisfies $1 < c < 2$. As in the proof of Lemma 2.1, we can arrive at (1). Hence c is a root of the polynomial equation $g(x) = 0$. To complete the proof of the "only if" part, we only need to show that $a < 2b$. To do this look at

$$g'(x) = ax^{a-1} - 2bx^{b-1} = x^{b-1}(ax^{a-b} - 2b), \qquad (2)$$

and $g'(1) = a - 2b$. If $a \geq 2b$, then (2) shows that $g'(x) > 0$ for $1 < x < 2$ and so $g(x)$ is increasing on the interval $(1,2)$. But $g(1) = 0$. Hence $g(x) > 0$ for all $x \in (1,2)$, whence $g(x)$ has no root in $(1,2)$, a contradiction. Thus, for c to exist such that $g(c) = 0$ and $c \in (1,2)$, we need to have $a < 2b$.

Now, conversely, let $c > 1$ and suppose that

$$c^a - 2c^b + 1 = 0$$

where a and b are positive integers and $b < a < 2b$. Let $n_1 = 0$, $n_2 = b$, $n_3 = a$. Then $n_1 < n_2 < n_3$ and

$$c^{n_3} - 2c^{n_2} + c^{n_1} = 0$$

or

$$c^{n_3} - c^{n_2} = c^{n_2} - c^{n_1} .$$

Hence $c^{n_1}, c^{n_2}, c^{n_3}$ are three terms in arithmetic progression. (That is, $1, c^b, c^a$ are three terms in arithmetic progression. Note that c^k, c^{b+k}, c^{a+k} are also in arithmetic progression for all $k \geq 0$). This proves the theorem completely.

In the polynomial $g(x) = x^a - 2x^b + 1$, it is impossible, when $b = 1$, to find an integer a such that $b < a < 2b$. Hence we may assume that $1 < b < a < 2b$.

Example 1. Let $a = 3$, $b = 2$, we will find c , $1 < c < 2$ such that $1, c^2, c^3$ are in arithmetic progression. To do this, let

$$f(x) = x^3 - 2x^2 + 1 .$$

Since 1 is a root of $f(x) = 0$, we can factor $f(x)$ and get

$$f(x) = (x-1)(x^2-x-1).$$

We need only to find the roots of $x^2 - x - 1 = 0$. These roots are $x = \frac{1 \pm \sqrt{5}}{2}$. But since $1 < c < 2$, it follows that $c = \frac{1 + \sqrt{5}}{2}$. Therefore 1, $(\frac{1 + \sqrt{5}}{2})^2$, $(\frac{1 + \sqrt{5}}{2})^3$ are in arithmetic progression. To check that:

$$(\frac{1 + \sqrt{5}}{2})^2 - 1 = \frac{3 + \sqrt{5}}{2} - 1 = \frac{1 + \sqrt{5}}{2}$$

and

$$(\frac{1 + \sqrt{5}}{2})^3 - (\frac{1 + \sqrt{5}}{2})^2 = (\frac{1 + \sqrt{5}}{2})^2(\frac{1 + \sqrt{5}}{2} - 1) = \frac{3 + \sqrt{5}}{2}(\frac{-1 + \sqrt{5}}{2}) = \frac{1 + \sqrt{5}}{2}.$$

This seems to be the simplest example of a geometric progression $\{c^n\}$ which contains a three term arithmetic progression.

Example 2. Let $a = 4$, $b = 3$, $f(x) = x^4 - 2x^3 + 1$. Since 1 is a root of the polynomial equation $f(x) = 0$, we factor and get $f(x) = (x-1)(x^3 - x^2 - x - 1) = 0$. We need only to solve $x^3 - x^2 - x - 1 = 0$. We follow the method for solving cubics as outlined in [2, page 17]. Then we have $a_0 = a_1 = a_2 = -1$, where $x^3 + a_2x^2 + a_1x + a_0 = 0$,

$$q = \frac{1}{3}a_1 - \frac{1}{9}a_2^2 = -\frac{1}{3} - \frac{1}{9} = -\frac{4}{9},$$

$$r = \frac{1}{6}(a_1a_2 - 3a_0) - \frac{1}{27}a_2^3 = \frac{1}{6}(1 + 3) + \frac{1}{27} = \frac{19}{27},$$

$$q^3 + r^2 = -\frac{64}{729} + \frac{361}{729} = \frac{297}{729} > 0 .$$

So there is one real root and a pair of complex conjugate roots. Now

$$S_1 = [r + (q^3 + r^2)^{\frac{1}{2}}]^{1/3} = (\frac{19 + \sqrt{297}}{27})^{1/3} = \frac{1}{3}(19 + \sqrt{297})^{1/3}$$

$$S_2 = [r - (q^3 + r^2)^{\frac{1}{2}}]^{1/3} = (\frac{19 - \sqrt{297}}{27})^{1/3} = \frac{1}{3}(19 - \sqrt{297})^{1/3} .$$

So the real root $c = S_1 + S_2 - \frac{a_2}{3} = \frac{1}{3}[19 + \sqrt{297})^{1/3} + (19 - \sqrt{297})^{1/3} + 1]$ $\doteq 1.839286755$. Thus, 1, $(1.839286755)^3$, $(1.839286755)^4$ are in arithmetic progression with a difference approximately equal to 5.2226252.

It is amazing that this c appears to be the second simplest such solution (after the simplest $c = \frac{1 + \sqrt{5}}{2}$) which we have found.

Define

$S = \{c: 1 < c < 2$ and $\{c^n\}$ has a 3-term arithmetic progression$\}$.

Theorem 2.3. Let $\varepsilon = 2^{1/t}$, $t = 2,3,4,\ldots$. Then $\varepsilon \notin S$.

Before we give the proof of Theorem 2.3. We introduce the following fact from algebra [3, see page 320].

Lemma 2.4. If $\varepsilon = 2^{1/t}$, $t > 1$ is an integer, then $1,\varepsilon,\varepsilon^2,\varepsilon^3,\ldots,\varepsilon^{t-1}$ are linearly independent over the field of rational numbers. [That is, if $r_0 + r_1\varepsilon + r_2\varepsilon^2 + \ldots + r_{t-1}\varepsilon^{t-1} = 0$, r_i is

rational number, then $r_0 = r_1 = r_2 = \ldots = r_{t-1} = 0$, or again, ε is not a root of any polynomial with rational coefficient of degree less than t since x^t-2 is clearly the irreducible polynomial for ε over the rationals.]

Proof of Theorem 2.3. Suppose, on the contrary, that $\varepsilon \in S$, where $\varepsilon = 2^{1/t}$ for some t. Then by Theorem 2.2 we have

$$\varepsilon^a - 2\varepsilon^b + 1 = 0$$

where a and b are integers and $1 < b < a < 2b$. That is, we have

$$(2^{1/t})^a - 2(2^{1/t})^b + 1 = 0 .$$

Let $a = qt + r$, $0 \le r < t$

and

$$b = q't + r' , \quad 0 \le r' < t .$$

Then we have

$$(2^{1/t})^{qt+r} - 2(2^{1/t})^{q't+r'} + 1$$

$$= 2^q(2^{1/t})^r - 2^{q'+1}(2^{1/t})^{r'} + 1$$

$$= 2^q\varepsilon^r - 2^{q'+1}\varepsilon^{r'} + 1 = 0 . \qquad (2)$$

Since $r < t$, $r' < t$, then by Lemma 2.4, we have $2^q - 2^{q'+1} + 1 = 0$ a contradiction. Hence $\varepsilon \notin S$.

Let $f_{a,b}(x) = x^a - 2x^b + 1$, $1 < b < a < 2b$. Then for each polynomial $f_{a,b}$ there corresponds a unique $c_{a,b}$ in S such that

$$f_{a,b}(c_{a,b}) = 0 .$$

But since we have only countably many such polynomials (because I x I is countable), it follows that we have only countably many $c_{a,b}$'s in S. Hence S is a countable set. It will follow from Theorem 2.6 below that S is infinite.

Lemma 2.5. Let $f(x) = x^a - 2x^b + 1$, $1 < b < a < 2b$ and $f(c) = 0$, where $1 < c < 2$. Then

$$1 < (\frac{2b}{a})^{\frac{1}{a-b}} < c < 2^{\frac{1}{a-b}} .$$

Proof. $f'(x) = ax^{a-1} - 2bx^{b-1} = x^{b-1}[ax^{a-b} - 2b]$. It follows that $f'(x) = 0$, when $x = (\frac{2b}{a})^{\frac{1}{a-b}}$. Now $f'(1) = a - 2b < 0$, $f(1) = 0$, $f(2) = 2^a - 2^{b+1} + 1 > 0$, $f'(x) < 0$ for $1 \le x < (\frac{2b}{a})^{\frac{1}{a-b}}$, and $f'(x) > 0$ for $(\frac{2b}{a})^{\frac{1}{a-b}} < x \le 2$. These facts allow us to graph $f(x)$ as in Figure 1.

Since $f(c) = 0$, $f(1) = 0$, it is clear that

$$1 < (\frac{2b}{a})^{\frac{1}{a-b}} < c .$$

Next, we want to show that $c < 2^{\frac{1}{a-b}}$. Since

$$f(2^{\frac{1}{a-b}}) = 2^{\frac{a}{a-b}} - 2.2^{\frac{b}{a-b}} + 1$$

$$= 2^{\frac{b}{a-b}}[2-2] + 1 = 1 > 0 .$$

Then $c < 2^{\frac{1}{a-b}}$.

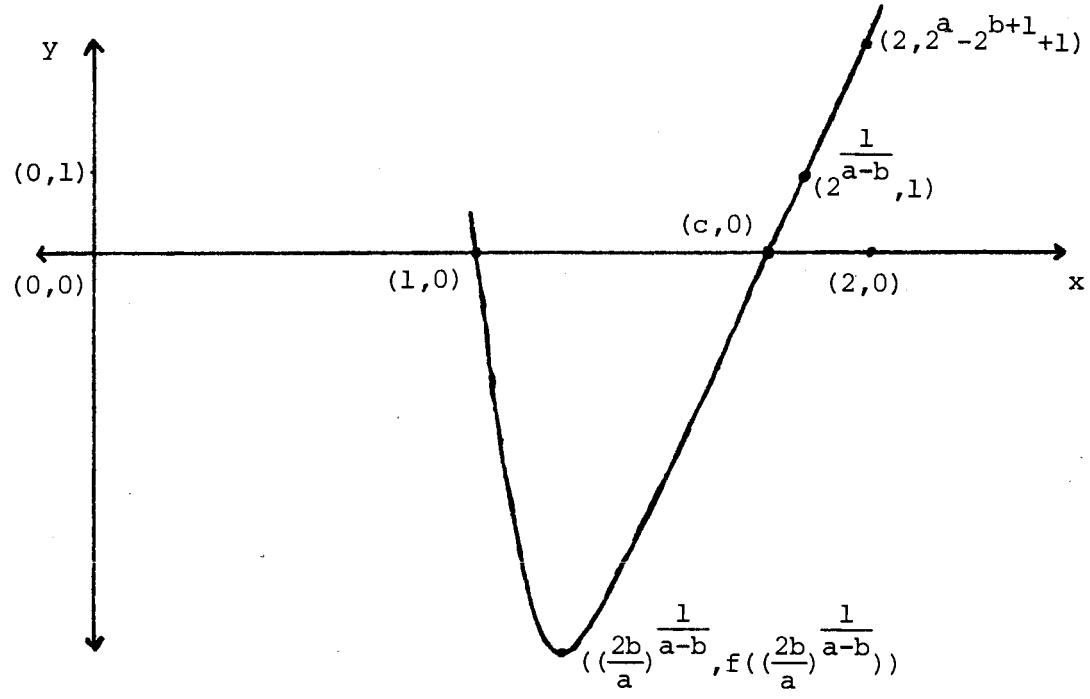

Figure 1

Theorem 2.6. Let $T = \{\ell: \ell = 1$ or $\ell = 2^{1/t}$ for some integer $t \geq 1\}$. Then T = the set of all cluster points of S .

Proof. Let ε be a cluster point of S . Then $c_{a_n,b_n} \to \varepsilon$ ($c_{a_n,b_n} \neq \varepsilon$ for all n), $f_n(c_{a_n,b_n}) = 0$, where $f_n(x) = x^{a_n} - 2x^{b_n} + 1$, $1 < b_n < a_n < 2b_n$. It follows that a_n and b_n are unbounded (since otherwise there are only finitely many c_{a_n,b_n}). Hence we may assume that $a_n \to \infty$ (and therefore $b_n \to \infty$).

By virtue of Lemma 2.5, we have

$$1 < \left(\frac{2b_n}{a_n}\right)^{\frac{1}{a_n - b_n}} < c_{a_n,b_n} < 2^{\frac{1}{a_n - b_n}} .$$

So two cases follow.

Case 1. If $a_n - b_n$ is arbitrarily large, then the c_{a_n,b_n} come arbitrarily close to 1 (since $2^{\frac{1}{a_n - b_n}}$ is arbitrarily close to 1) and so $\varepsilon = 1$.

Case 2. If $a_n - b_n$ is bounded, say $a_n - b_n = t$ (infinitely often). Then

$$\left(\frac{2b_n}{a_n}\right)^{1/t} = \left(\frac{2a_n - 2t}{a_n}\right)^{1/t} = \left(2 - \frac{2t}{a_n}\right)^{1/t}$$

is arbitrarily close to $2^{1/t}$ since $a_n \to \infty$. But c_{a_n,b_n} is such that $\left(\frac{2b_n}{a_n}\right)^{1/t} < c_{a_n,b_n} < 2^{1/t}$. So we have that some c_{a_n,b_n} come arbitrarily close to $2^{1/t}$ and so $c_{a_n,b_n} \to 2^{1/t}$. Hence $\varepsilon = 2^{1/t}$. Thus the set of all cluster points of S is contained in T.

Now, we want to show that T is contained in the set of all cluster points of S. That is, if $\varepsilon = 1$ or $\varepsilon = 2^{1/t}$ for some integer $t \geq 1$, then we show that there exists c_{a_n,b_n} in S such that $c_{a_n,b_n} \to \varepsilon$. To do this, let $f_n(x) = x^{a_n} - 2x^{b_n} + 1$, where $1 < b_n < a_n < 2b_n$.

(i) Let $\varepsilon = 1$ and let $b_n = n$ and $a_n = 2n - 1$. It follows that for each $n \geq 2$, there exists c_{a_n,b_n} in S, and by Lemma 2.5, we have

$$1 < \left(\frac{2b_n}{a_n}\right)^{\frac{1}{a_n - b_n}} < c_{a_n,b_n} < 2^{\frac{1}{a_n - b_n}}.$$

That is,

$$1 < \left(\frac{2n}{2n-1}\right)^{\frac{1}{n-1}} < c_{a_n,b_n} < 2^{\frac{1}{n-1}},$$

which implies that $c_{a_n,b_n} \to 1$ as $n \to \infty$.

(ii) Let $\varepsilon = 2^{1/t}$, $t \geq 1$ and let $b_n = n$, $a_n = n + t$. It follows that for each $n \geq t+1$, there exists c_{a_n,b_n} in S. By Lemma 2.5, we have

$$1 < \left(\frac{2b_n}{a_n}\right)^{\frac{1}{a_n - b_n}} < c_{a_n,b_n} < 2^{\frac{1}{a_n - b_n}}.$$

That is,

$$1 < \left(\frac{2n}{n+t}\right)^{1/t} < c_{a_n,b_n} < 2^{1/t}, \quad 1 \leq t < n$$

which implies that $c_{a_n,b_n} \to 2^{1/t}$ as $n \to \infty$.

Corollary 2.7. The set S is nowhere dense in $(1,2)$.

Proof. If S is dense in some interval, then every point of this interval is a cluster point of S. In particular S would have an uncountable number of cluster points. Theorem 2.6 shows that S has only countably many cluster points.

Unfortunately, we have not been able to solve the problem of four-term arithmetic progressions in the geometric progression $\{c^n\}$. It is unlikely that any exist for any c. If $\{c^n\}$ contains a four-term arithmetic progression, then there are integers n_1, n_2, n_3, n_4 such that

$$c^{n_1}, c^{n_2}, c^{n_3}, c^{n_4}$$

in an arithmetic progression. It follows that c is a root of both the polynomials

$$x^a - 2x^b + 1 = 0$$

$$x^{a'} - 2x^{b'} + 1 = 0 ,$$

where $a = n_3 - n_1$, $b = n_2 - n_1$, $a' = n_4 - n_2$, $b' = n_3 - n_2$. One shows that $a > a'$, $b > b'$ and in fact $b' = a-b$. But even with these facts we cannot prove that the two equations do not have a simultaneous solution in the interval $(1,2)$.

CHAPTER 3

ARITHMETIC PROGRESSIONS IN QUADRATICS

In this Chapter we want to consider 3-term arithmetic progressions among quadratics.

Definition 3.1. The integers x,y,z are said to be a pythagorean triple if x,y,z, satisfy the equation

$$x^2 + y^2 = z^2 . \tag{1}$$

Remark 3.2. Suppose x,y,z is such a triple and $(x,y,z) = d$. If we put $x = dx_1$, $y = dy_1$, $z = dz_1$, we see that x_1,y_1,z_1 is also a pythagorean triple and $(x_1,y_1,z_1) = 1$. On the other hand if x,y,z is any solution of (1) and k is any integer, then kx,ky,kz is also a solution. Thus, any solution of (1) may be used to find a solution x,y,z such that $(x,y,z) = 1$, and conversely, a solution x,y,z with $(x,y,z) = 1$ may be used to generate a family of solutions.

Definition 3.3. A pythagorean triple x,y,z such that $(x,y,z) = 1$ is called a primitive pythagorean triple.

To find all solutions of (1), the above remark indicates that, it suffices to find all primitive solutions of (1). We confine our attention to the cases $x > 0$, $y > 0$, $z > 0$.

Lemma 3.4. If x,y,z is a primitive positive solution of (1), then $(x,y) = (x,z) = (y,z) = 1$.

Proof. To show that $(x,y) = 1$, suppose a prime p divides both x and y. Then $p^2|x^2$, $p^2|y^2$, it follows that $p^2|x^2 + y^2$. So $p^2|z^2$ and hence $p|z$, a contradiction. Therefore $(x,y) = 1$. The arguments are similar to show that $(x,z) = (y,z) = 1$.

Lemma 3.5. If x,y,z is a primitive positive solution of (1). Then x,y have opposite parity (one of the x and y is even and the other is odd).

Proof. By virtue of Lemma 3.4, both x and y cannot be even. To show that both x and y cannot be odd, assume that both x and y are odd. Then $x^2 \equiv 1 \pmod 4$ and $y^2 \equiv 1 \pmod 4$. So that $x^2 + y^2 \equiv 2 \pmod 4$ which is impossible since every square is congruent to either 0 or $1 \pmod 4$. Thus x and y have opposite parity.

Theorem 3.6. Assume x is even and y is odd. Then the positive primitive solutions of (1) are

$$x = 2rs,\ y = s^2 - r^2,\ z = s^2 + r^2,$$

where r,s are integers such that $0 < r < s$, $(r,s) = 1$ and r and s are of opposite parity.

Proof. See Gioia [4, page 121].

Corollary 3.7. There are infinitely many positive primitive solutions of (1).

Proof. If y and z are given, then r^2, s^2 and consequently r,s are uniquely determined. So that different values of x,y and z

corresponds to different values of r and s. Also, since there are infinitely many such values, then (1) has infinitely many positive primitive solutions.

Define $I^2 = \{i^2 : i = 1,2,3,\ldots\}$. We will consider 3-term arithmetic progressions in I^2.

We call a 3-term arithmetic progression a,b,c primitive if $(a,b,c) = 1$.

Lemma 3.8. If a^2,b^2,c^2 is a primitive 3-term arithmetic progression in I^2. Then $(a,b) = (b,c) = (a,c) = 1$.

Proof. We have $a^2 + c^2 = 2b^2$ and $(a^2,b^2,c^2) = 1$, where $0 < a < b < c$, a,b,c are integers. To show that $(a,b) = 1$, suppose a prime p divides both a and b. Then $p|a^2$, $p|b^2$. It follows that $p|2b^2$ and $p|2b^2 - a^2$. Hence $p|c^2$, a contradiction. By a similar argument we can show that $(b,c) = 1$.

Next, to show that $(a,c) = 1$, suppose a prime p divides both a and c. Then $p|a^2$, $p|c^2$. Hence $p|a^2 + c^2$. So that $p|2b^2$. It follows that either $p|b^2$, a contradiction, or $p = 2$ which implies that both a and c are even. Hence $4|a^2 + c^2$. So $4|2b^2$ which implies that $2|b^2$, again, a contradiction.

Theorem 3.9. x,y,z is a primitive pythagorean triple if and only if $(x-y)^2$, z^2, $(x+y)^2$ is a primitive 3-term arithmetic progression in I^2.

Proof. Suppose x,y,z is a primitive pythegorean triple. Then $x^2 + y^2 = z^2$. But

$$(x-y)^2 + (x+y)^2 = x^2 - 2xy + y^2 + x^2 + 2xy + y^2$$

$$= 2(x^2 + y^2)$$

$$= 2z^2 .$$

Hence $(x-y)^2$, z^2, $(x+y)^2$ is a 3-term arithmetic progression. To show it is primitive suppose a prime p divides $(x-y)^2$, z^2 and $(x+y)^2$. Then $p|x-y$, $p|x+y$. It follows that $p|2x$, $p|2y$. Hence either $p = 2$ or $p|x$, $p|y$. Since, by Lemma 3.4, $(x,y) = 1$, we have $p = 2$. So $2|x+y$ which implies that x and y have same parity which contradicts Lemma 3.5.

Conversely, suppose that $(x-y)^2$, z^2, $(x+y^2)^2$ is a primitive 3-term arithmetic progression. Then

$$(x-y)^2 + (x+y)^2 = 2z^2 .$$

But,

$$(x-y)^2 + (x+y)^2 = x^2 - 2xy + y^2 + x^2 + 2xy + y^2$$

$$= 2(x^2+y)^2 .$$

Hence $x^2 + y^2 = z^2$, whence x,y,z is a pythagorean triple. To show that x,y,z is a primitive pythagorean triple, suppose that a prime p divides x,y and z. Then $p|x-y$, $p|x+y$ which contradicts Lemma 3.8.

Example 3. Given $x = 4$, $y = 3$. It follows, when $z = 5$, that (x,y,z) is a primitive pythagorean triple. $(x-y)^2 = 1$, $z^2 = 25$,

$(x+y)^2 = 49$. But since $1 + 49 = 2.25$, $(1,25,49) = 1$. Then $1^2, 5^2, 7^2$ is a primitive 3-term arithmetic progression.

Example 4. Given $(7)^2, (13)^2, (17)^2$ a primitive 3-term arithmetic progression. To find x,y,z put $z = 13$, $x-y = 7$, $x+y = 17$. It follows that $x = 12$, $y = 5$. So $x^2+y^2 = (12)^2 + (5)^2 =$ $= (13)^2 = z^2$. Also $(12,5,13) = 1$. Therefore 12, 5, 13 is a primitive pythegorean triple.

Corollary 3.7 says that there are infinitely many positive primitive pythagorean triples. It yields by Theorem 3.9 that there are infinitely many primitive 3-term arithmetic progressions in I^2. Moreover, since a primitive pythagorean triple x,y,z can generate a family of pythagorean triples, say kx,ky,kz, where k is a positive integer. It follows that $k^2(x-y)^2, k^2(z^2), k^2(x+y)^2$ is a family of 3-term arithmetic progression generated by $(x-y)^2, z^2, (x+y)^2$.

Theorem 3.10. a^2,b^2,c^2 is a primitive 3-term arithmetic progression with $0 < a < b < c$ if and only if the following are satisfied

$$a = x-y,\ b = z,\ c = x+y\ , \tag{2}$$

where $x = \max\{2rs, s^2 - r^2\}$, $y = \min\{2rs, s^2 - r^2\}$, $z = r^2 + s^2$, r and s are integers such that $0 < r < s$, $(r,s) = 1$ and r and s are of opposite parity.

Proof. Suppose a^2,b^2,c^2 is a primitive 3-term arithmetic progression. Then

$$a^2 + c^2 = 2b^2$$

where $(a^2,b^2,c^2) = 1$, $0 < a < b < c$ and a,b,c are integers. Since $a^2 + c^2$ is even, it follows that a^2,c^2 and hence a,c have same parity. $\frac{c+a}{2} = x$, $\frac{c-a}{2} = y$ are both integers. This yields that $x-y = a$, $x+y = c$, $0 < y < x$. But

$$a^2 + c^2 = (x-y)^2 + (x+y)^2 = 2(x^2+y^2) = 2b^2 .$$

Let $z = \sqrt{x^2+y^2}$, then $z = b$. Therefore we have that $(x-y)^2$, z^2, $(x+y)^2$ is a primitive 3-term arithmetic progression in I^2. Hence, by virtue of Theorem 3.9, x,y,z is a primitive pythagorean triple. So Theorem 3.6 implies, (since $x > y$), that

$$x = \max\{2rs, s^2 - r^2\} , y = \min\{2rs, s^2 - r^2\} , z = s^2 + r^2 ,$$

where r,s are integers, $0 < r < s$, $(r,s) = 1$ and r,s are of opposite parity. Thus conditions (2) are satisfied.

Conversely, suppose we have (2) and we wish to show that a^2,b^2,c^2 is a primitive 3-term arithmetic progression. Since $0 < r < s$. It follows $2rs > 0$, $s^2-r^2 > 0$, $r^2+s^2 > 0$ and hence $x > 0$, $y > 0$, $z > 0$. We claim that $x \neq y$. To see this assume, on the contrary, that $x = y$ or equivalently assume $s^2 - r^2 = 2sr$ which implies that $(s-r)^2 = 2r^2$. It follows that $\frac{s-r}{r} = \sqrt{2}$ an irrational, a contradiction. Hence $x > y > 0$. From Theorem 3.6, it yields that x,y,z is a primitive pythagorean triple (i.e., $x^2 + y^2 = z^2$, $(x,y,z) = 1$). Therefore, by virtue of Theorem

3.9, $(x-y)^2$, z^2, $(x+y)^2$ is a primitive 3-term arithmetic progression. Thus, a^2, b^2, c^2 is a primitive 3-term arithmetic progression. The proof of the theorem is complete.

Define $f(n) = (n+t)^2$, where $n \geq -t$ is an integer and t is a fixed real number.

Theorem 3.11. If t is an irrational number, then $\{f(n)\}$ has no 3-term arithmetic progression.

Proof. Suppose, on contrary, that $\{f(n)\}$ has a 3-term arithmetic progression. Then, for $n_1 < n_2 < n_3$, we have

$$(n_1+t)^2 + (n_3+t)^2 = 2(n_2+t)^2$$

or

$$n_1^2 + 2n_1t + t^2 + n_3^2 + 2n_3t + t^2 = 2(n_2^2 + 2n_2t + t^2),$$

so

$$n_1^2 + n_3^2 - 2n_2^2 = t(4n_2 - 2n_1 - 2n_3). \tag{3}$$

We claim that $4n_2 - 2n_1 - 2n_3 \neq 0$. To prove this, suppose that $4n_2 - 2n_1 - 2n_3 = 0$. It follows that $n_1 + n_3 = 2n_2$. So that n_1, n_2, n_3 is a 3-term arithmetic progression. Hence $n_2 = n_1+d$, $n_3 = n_1+2d$, where d is a positive integer. Again, it follows from (3) that $n_1^2 + n_3^2 - 2n_2^2 = 0$. Therefore we have

$$n_1^2 + (n_1+2d)^2 = 2(n_1+d)^2$$

or

$$n_1^2 + n_1^2 + 4n_1d + 4d^2 = 2n_1^2 + 4n_1d + 2d^2$$

which implies that $2 = 1$. This absurdity implies that

$$4n_2 - 2n_1 - 2n_3 \neq 0 \ .$$

Hence we can write

$$t = \frac{n_1^2 + n_3^2 - 2n_2^2}{4n_2 - 2n_1 - 2n_3}$$

a rational number. This contradiction completes the proof.

Corollary 3.12. If $\{f(n)\}$ has a 3-term arithmetic progression. Then t is a rational number.

Theorem 3.13. Let $t = \frac{b}{a}$, where a, b are integers, $a \neq 0$. Let $f(n) = (n+t)^2$, $g(n) = (an+b)^2$. Then $f(n_1)$, $f(n_2)$, $f(n_3)$ is a 3-term arithmetic progression with $-t \leq n_1 < n_2 < n_3$ if and only if $g(n_1)$, $g(n_2)$, $g(n_3)$ is the same.

Proof. We consider the increasing part of f and g only. Hence let $g(n_1)$, $g(n_2)$, $g(n_3)$ be a 3-term arithmetic progression with $\frac{-b}{a} \leq n_1 < n_2 < n_3$. Then we have

$$(an_1+b)^2 + (an_3+b)^2 = 2(an_2+b)^2$$

or

$$a^2(n_1+\frac{b}{a})^2 + a^2(n_3+\frac{b}{a})^2 = 2a^2(n_2+\frac{b}{a})^2$$

which implies that

$$(n_1+t)^2 + (n_3+t)^2 = 2(n_2+t)^2 .$$

Hence $f(n_1)$, $f(n_2)$, $f(n_3)$ is a 3-term arithmetic progression.

By a similar argument we can prove the converse.

Theorem 3.14. Let $h(n) = \alpha n^2 + \beta n + \gamma$ where α,β,γ are reals, $\alpha > 0$. Let $f(n) = (n+t)^2$ where $t = \beta/2\alpha$. Then $h(n_1)$, $h(n_2)$, $h(n_3)$ is a 3-term arithmetic progression with $\frac{-\beta}{2\alpha} \le n_1 < n_2 < n_3$ if and only if $f(n_1)$, $f(n_2)$, $f(n_3)$ is the same.

Proof. Suppose $h(n_1) < h(n_2) < h(n_3)$ is a 3-term arithmetic progression with $\frac{-\beta}{2\alpha} \le n_1 < n_2 < n_3$. Then we have

$$(\alpha n_1^2 + \beta n_1 + \gamma) + (\alpha n_3^2 + \beta n_3 + \gamma) = 2(\alpha n_2^2 + \beta n_2 + \gamma)$$

$$(\alpha n_1^2 + \beta n_1) + (\alpha n_3^2 + \beta n_3) = 2(\alpha n_2^2 + \beta n_2)$$

$$(n_1^2 + (\beta/\alpha)n_1) + (n_3^2 + (\beta/\alpha)n_3) = 2(n_2^2 + (\beta/\alpha)n_2)$$

$$(n_1^2 + (\beta/\alpha)n_1 + (\beta/2\alpha)^2) + (n_3^2 + (\beta/\alpha)n_3 + (\beta/2\alpha)^2) = 2(n_2^2 + (\beta/\alpha)n_2 + (\beta/2\alpha)^2)$$

$$(n_1 + \beta/2\alpha)^2 + (n_3 + \beta/2\alpha)^2 = 2(n_2 + \beta/2\alpha)^2$$

and finally

$$(n_1 + t)^2 + (n_3 + t)^2 = 2(n_2 + t)^2$$

which implies that $f(n_1) < f(n_2) < f(n_3)$ is a 3-term arithmetic progression.

By reversing the above steps we can prove the converse.

Corollary 3.15. If $\{h(n)\}$ has a 3-term arithmetic progression, then β/α is a rational.

Proof. The proof follows from 3.14 and 3.12.

We will consider functions of the form

$$h(n) = \alpha n^2 + \beta n + \gamma, \tag{4}$$

where α,β,γ are reals, $\alpha > 0$ and n is non-negative integer. suppose $\{h(n)\}$ has a 3-term arithmetic progression $h(n_1) < h(n_2) < h(n_3)$, where $\frac{-\beta}{2\alpha} \leq n_1 < n_2 < n_3$. It follows, by virtue of Theorem 3.14, that $f(n_1) < f(n_2) < f(n_3)$ is a 3-term arithmetic progression, where $f(n) = (n+t)^2$ and $t = \beta/2\alpha$. But t is a rational, say $t = \frac{b}{a}$ where a and b are integers and $a > 0$. Then Theorem 3.13 implies that $g(n_1), g(n_2), g(n_3)$ is a 3-term arithmetic progression, where $g(n) = (an + b)^2$. That is, we have

$$(an_1 + b)^2 + (an_3 + b)^2 = 2(an_2 + b)^2 .$$

By the division algorithm we can write $b = ak + b'$, where k and b' are integers and $0 \leq b' < a$. Hence, by substitution

$$(an_1' + b')^2 + (an_3' + b')^2 = 2(an_2' + b')^2 , \tag{5}$$

where $0 \le b' < a$ and $n_i' = n_i + k$, $i = 1,2,3$.
Moreover, if $(a,b') = d > 1$, then $a = a_1 d$, $b' = b_1 d$ and $(a_1,b_1) = 1$ and so (5) becomes

$$d^2(a_1 n_1' + b_1)^2 + d^2(a_1 n_3' + b_1)^2 = 2d^2(a_1 n_2' + b_1)^2$$

which implies that $\{(a_1 n + b_1)^2\}$ has a 3-term arithmetic progression.

Note that, the converse of these arguments are also valid. Hence we can conclude that, to study 3-term arithmetic progressions in the quadratics in (4), it suffices to study 3-term arithmetic progressions in $\{(an + b)^2\}$, where a and b are integers, $0 \le b < a$ and $(a,b) = 1$. We will consider <u>primitive</u> 3-term arithmetic progressions in $\{(an + b)^2\}$.

We <u>define</u> $T = \{(a,b)$: a and b are integers, $a > b \ge 0$, $(a,b) = 1$ and $\{(an + b)^2\}$ contains a <u>primitive</u> 3-term arithmetic progression$\}$.

It is clear that $(1,0) \in T$, since I^2 contains infinitely many primitive 3-term arithmetic progressions. Hence to study whether or not $(a,b) \in T$, we need only to study the cases where $a > b > 0$, $(a,b) = 1$. First we study the case when a is an <u>odd number</u>, and we have the following long theorem.

<u>Theorem 3.16</u>. Let a be an odd number, b be an integer such that $a > b > 0$, $(a,b) = 1$. Then $(a,b) \in T$ if and only if b, $\frac{b}{2}$ or $\frac{b+a}{2}$ is a quadratic residue modulo a.

Proof. Suppose $(a,b) \in T$. From the definition of T, there exist integers $0 \leq n_1 < n_2 < n_3$ such that $(an_1 + b)^2$, $(an_2 + b)^2$, $(an_3 + b)^2$ is a primitive 3-term arithmetic progression. By virtue of Theorem 3.10, we have

$$\begin{aligned} an_1 + b &= x - y \\ an_2 + b &= z \\ an_3 + b &= x + y , \end{aligned} \tag{6}$$

where $x = \max\{2rs, s^2 - r^2\}$, $y = \min\{2rs, s^2 - r^2\}$, $z = s^2 + r^2$, r and s are integers such that $s > r > 0$, $(r,s) = 1$ and r and s are of opposite parity. Equations(6) mean that

$$\begin{aligned} x - y &\equiv b \pmod{a} \\ z &\equiv b \pmod{a} \\ x + y &\equiv b \pmod{a}. \end{aligned}$$

It follows that

$$\begin{aligned} 2x &\equiv 2b \pmod{a} \\ z &\equiv b \pmod{a} \\ 2y &\equiv 0 \pmod{a} \end{aligned}$$

since $(a,2) = 1$, then

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

$$z \equiv b \pmod{a} \qquad (7)$$

$$y \equiv 0 \pmod{a}.$$

Now we have two cases:

Case 1. $x = s^2 - r^2$, $y = 2rs$, $z = s^2 + r^2$.

In this case (7) becomes

$$s^2 - r^2 \equiv b \pmod{a}$$

$$s^2 + r^2 \equiv b \pmod{a}$$

$$2rs \equiv 0 \pmod{a}$$

which implies that

$$2s^2 \equiv 2b \pmod{a}$$

$$2r^2 \equiv 0 \pmod{a}$$

$$2rs \equiv 0 \pmod{a}.$$

Again, since $(a,2) = 1$, $s^2 \equiv b \pmod{a}$, and hence b is a quadratic residue mod a.

Case 2. $x = 2rs$, $y = s^2 - r^2$, $z = s^2 + r^2$. In this case (7) becomes

$$2rs \equiv b \pmod{a}$$

$$s^2 + r^2 \equiv b \pmod{a}$$

$$s^2 - r^2 \equiv 0 \pmod{a}$$

which implies that

$$2rs \equiv b \pmod{a}$$

$$2r^2 \equiv b \pmod{a}$$

$$2s^2 \equiv b \pmod{a} \ .$$

Again, since $(a,2) = 1$. It follows that, if b is even, then, e.g., $r^2 \equiv \frac{b}{2} \pmod{a}$, and hence $\frac{b}{2}$ is a quadratic residue mod a. If b is odd, then we get $r^2 \equiv \frac{a+b}{2} \pmod{a}$, and hence $\frac{a+b}{2}$ is a quadratic residue mod a. This completes the proof in the forward direction.

Conversely, let a be an odd number, b be an integer such that $a > b > 0$, $(a,b) = 1$.

(i) Suppose b is a quadratic residue modulo a. Then there exists a positive integer t such that $t^2 \equiv b \pmod{a}$. Let $r = a$, $s = t + ka$, then $s^2 \equiv t^2 \equiv b \pmod{a}$. So that r is odd and s is even when t and k have the same parity. We show $(r,s) = 1$. Suppose not: let p be a prime such that $p|r$, $p|s$. It follows that $p|a$ and $p|t$. But, $a|t^2 - b$. Hence $p|t^2 - b$, whence $p|b$, a contradiction since $(a,b) = 1$. Next,

$$s^2 - r^2 = (t + ka)^2 - a^2$$
$$= t^2 + 2kat + (k^2 - 1)a^2 ,$$

$$2rs = 2a(t + ka)$$
$$= 2at + 2ka^2 .$$

It is clear that for $k \geq 3$, we have $s^2 - r^2 > 2rs$. Hence, for $k \geq 3$ and k and t having the same parity, we have $s > r > 0, (r,s) = 1$, r and s are of opposite parity, $s^2 - r^2 > 2rs$ and

$$s^2 \equiv b \pmod{a}$$

$$r^2 \equiv 0 \pmod{a}$$

$$2rs \equiv 0 \pmod{a} ,$$

which implies that

$$s^2 - r^2 \equiv b \pmod{a}$$

$$s^2 + r^2 \equiv b \pmod{a}$$

$$2rs \equiv 0 \pmod{a} .$$

Let $x = s^2 - r^2$, $y = 2rs$, $z = s^2 + r^2$. Then x,y,z is a primitive pythagrean triple and

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

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

$$y \equiv 0 \pmod{a}.$$

It follows that

$$x - y \equiv b \pmod{a}$$

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

$$x + y \equiv b \pmod{a} .$$

That is,

$$x - y = an_1 + b$$

$$z = an_2 + b$$

$$x + y = an_3 + b ,$$

where clearly $0 \leq n_1 < n_2 < n_3$. By virtue of Theorem 3.10, $(x-y)^2$, z^2, $(x+y)^2$ and hence $(an_1+b)^2$, $(an_2+b)^2$, $(an_3+b)^2$ is a primitive 3-term arithmetic progression. Thus $(a,b) \in T$.

(ii) Suppose $\frac{b}{2}$ is a quadratic residue modulo a (where, of course, b is even). Then there exists a positive integer t such that $t^2 \equiv \frac{b}{2} \pmod{a}$. Let $r = t + ka$, $s = t + (k+1)a = r+a$. Then $s > r > 0$, r and s are of opposite parity and $s^2 \equiv r^2 \equiv rs \equiv \frac{b}{2} \pmod{a}$. We show $(r,s) = 1$. Suppose not: Let p be a prime such that $p|r$ and $p|s$. It follows $p|a$ and so $p|t$. But, since $a|t^2 - \frac{b}{2}$, then $p|t^2 - \frac{b}{2}$ which implies $p|b$, a contradiction since $(a,b) = 1$. Hence $(r,s) = 1$. Next,

$$2rs = 2(t + ka)(t + (k + 1)a)$$

$$= 2t^2 + 4kat + 2at + 2k^2a^2 + 2ka^2 ,$$

$$s^2 - r^2 = (t + (k + 1)a)^2 - (t + ka)^2$$

$$= 2at + 2ka^2 + a^2 .$$

It is clearly, for $k \geq 1$, that $2rs > s^2 - r^2$. Thus, for $k \geq 1$, we have $s > r > 0$, $(r,s) = 1$, r and s are of opposite parity, $2rs > s^2 - r^2$, and $s^2 \equiv r^2 \equiv rs \equiv \frac{b}{2} \pmod{a}$. It follows that

$$2rs \equiv b \pmod{a}$$

$$r^2 + s^2 \equiv b \pmod{a}$$

$$s^2 - r^2 \equiv 0 \pmod{a} .$$

Let $x = 2rs$, $y = s^2 - r^2$, $z = r^2 + s^2$. Then x,y,z is a primitive pythagorean triple, and

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

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

$$y \equiv 0 \pmod{a}$$

which implies, as before, that

$$x - y = an_1 + b$$

$$z = an_2 + b$$

$$x + y = an_3 + b$$

where, again, $0 \leq n_1 < n_2 < n_3$. Hence $(x-y)^2$, z^2, $(x+y)^2$, and so $(an_1+b)^2$, $(an_2+b)^2$, $(an_3+b)^2$ is a primitive 3-term arithmetic progression. Whence $(a,b) \in T$.

(iii) Finally, suppose $\frac{a+b}{2}$ is a quadratic residue modulo a (where, of course, b is odd). Then there exists a positive integer t such that $t^2 \equiv \frac{a+b}{2} \pmod{a}$. Let $r = t + ka$, $s = t + (k + 1)a = r + a$. It is clearly, as in (ii) above, that for $k \geq 1$ we have $s > r > 0$, $(r,s) = 1$, r and s are of opposite parity, $2rs > s^2 - r^2$ and $s^2 \equiv r^2 \equiv rs \equiv t^2 \equiv \frac{a+b}{2} \pmod{a}$. Which implies that

$$2rs \equiv b + a \equiv b \pmod{a}$$

$$2r^2 \equiv b + a \equiv b \pmod{a}$$

$$2s^2 \equiv b + a \equiv b \pmod{a}.$$

It follows, as in (ii), that

$$x - y = an_1 + b$$

$$z = an_2 + b$$

$$x + y = an_3 + b,$$

where $0 \leq n_1 < n_2 < n_3$. Hence $(x-y)^2$, z^2, $(x+y)^2$, and so $(an_1+b)^2$, $(an_2+b)^2$, $(an_3+b)^2$ is a primitive 3-term arithmetic progression. Thus $(a,b) \in T$. The proof of the Theorem is complete.

Now, we study the case when a is <u>even</u>. We have not been able to solve the problem completely in this case as we did for a odd.

<u>Theorem 3.17</u>. Let a be even and b be an integer such that $a > b > 0$, $(a,b) = 1$. If b is a quadratic residue modulo a, then $(a,b) \in T$.

<u>Proof</u>. Since b is a quadratic residue mod a, then there exists a positive integer t such that $t^2 \equiv b \pmod{a}$. But b is odd. It follows that t^2 and hence t is odd. Let $r = a$, $s = t + ka$. Then r is even and s is odd. We show $(r,s) = 1$. Suppose not: let a prime p divide both r and s. Then $p|a$ and $p|t$. But $a|t^2 - b$, it follows that $p|t^2 - b$ and hence $p|b$, a contradiction since $(a,b) = 1$. Next,

$$s^2 - r^2 = (t + ka)^2 - a^2 = t^2 + 2kat + (k^2 - 1)a^2 ,$$

$$2rs = 2a(t + ka) = 2at + 2ka^2 .$$

Thus, for $k \geq 3$, we have $s > r > 0$, $(r,s) = 1$, r and s are of opposite parity, $s^2 - r^2 > 2rs$ and

$$s^2 \equiv t^2 \equiv b \pmod{a}$$

$$r^2 \equiv 0 \pmod{a}$$

$$2rs \equiv 0 \pmod{a}.$$

which implies that

$$s^2 - r^2 \equiv b \pmod{a}$$

$$s^2 + r^2 \equiv b \pmod{a}$$

$$2rs \equiv 0 \pmod{a}.$$

Let $x = s^2 - r^2$, $y = 2rs$, $z = s^2 + r^2$. Then x,y,z is a primitive pythagorean triple. It follows, as before, that

$$x - y = an_1 + b$$

$$z = an_2 + b$$

$$x + y = an_3 + b$$

for some $0 \leq n_1 < n_2 < n_3$. Hence $(x-y)^2$, z^2, $(x+y)^2$ and whence $(an_1+b)^2$, $(an_2+b)^2$, $(an_3+b)^2$ is a primitive 3-term arithmetic progression. Thus $(a,b) \in T$.

Theorem 3.18. Let a be even such that $\frac{a}{2}$ is odd. Let b be such that $a > b > 0$ and $(a,b) = 1$. If $\frac{b + \frac{a}{2}}{2} = \frac{2b + a}{4}$ is a quadratic residue modulo a, then $(a,b) \in T$.

Proof. Since $\frac{2b+a}{4}$ is a quadratic residue mod a, then there exists a positive integer t such that $t^2 \equiv \frac{2b+a}{4} \pmod{a}$. Let $r = t + k\frac{a}{2}$, $s = t + (k+1)\frac{a}{2} = r + \frac{a}{2}$. Then r and s are of opposite parity since $\frac{a}{2}$ is odd. We want to show that $(r,s) = 1$. Suppose, on the contrary, that a prime p divides both r and s. Then p is an odd prime since r and s are of opposite parity and

$p|s-r$ (that is, $p|\frac{a}{2}$). Hence $p|a$ and $p|t$. But $a|t^2 - \frac{2b+a}{4}$, it follows that $p|t^2 - \frac{2b+a}{4}$ and so $p|\frac{2b+a}{4}$ which implies that $p|2b+a$. Because $p|a$ and p is an odd prime, then $p|b$ a contradiction since $(a,b) = 1$. Next,

$$2rs = 2(t + k\tfrac{a}{2})[t + (k+1)\tfrac{a}{2}]$$

$$= 2t^2 + 2kat + at + k^2\frac{a^2}{2} + k\frac{a^2}{2},$$

$$s^2 - r^2 = [t + (k+1)\tfrac{a}{2}]^2 - (t + k\tfrac{a}{2})^2$$

$$= at + k\frac{a^2}{2} + \frac{a^2}{4}.$$

It is clear, for $k \geq 1$, that we have $s > r > 0$, $(r,s) = 1$, $2rs > s^2 - r^2$ and r and s are of opposite parity.

Let $x = 2rs$, $y = s^2 - r^2$, $z = s^2 + r^2$. Then x,y,z is a primitive pythagorean triple. Hence by virtue of Theorem 3.10, $(x-y)^2$, z^2, $(x+y)^2$ is a primitive 3-term arithmetic progression. To complete the proof, we need only to show that

$$x - y \equiv z \equiv x + y \equiv b \pmod{a}.$$

(i) $x - y = 2rs - s^2 + r^2$

$$= 2(t + k\tfrac{a}{2})(t + (k+1)\tfrac{a}{2}) - (t + (k+1)\tfrac{a}{2})^2 + (t + k\tfrac{a}{2})^2$$

$$= 2t^2 + 2tka + k^2\frac{a}{2}a - \frac{a^2}{4}$$

$$\equiv 2t^2 - \frac{a^2}{4} \pmod{a}.$$

But, since $t^2 \equiv \frac{2b+a}{4} \pmod{a}$. Then

$$x - y \equiv b + \frac{a}{2} - \frac{a^2}{4} \equiv b + \frac{a}{2}(1 - \frac{a}{2}) \pmod{a}.$$

Since $\frac{a}{2}$ is odd, then $1 - \frac{a}{2}$ is even. Hence $x - y \equiv b \pmod{a}$.

(ii) $z = s^2 + r^2$

$$= (t + (k+1)\frac{a}{2})^2 + (t + k\frac{a}{2})^2$$

$$= 2t^2 + 2tka + ta + k^2 \frac{a}{2} a + k \frac{a}{2} a + \frac{a^2}{4}$$

$$\equiv 2t^2 + \frac{a^2}{4} \pmod{a}.$$

But, again, since $t^2 \equiv \frac{2b+a}{4} \pmod{a}$. It follows that

$$z \equiv b + \frac{a}{2} + \frac{a^2}{4} \equiv b + \frac{a}{2}(1 + \frac{a}{2}) \pmod{a}.$$

Since $\frac{a}{2}$ is odd, then $1 + \frac{a}{2}$ is even. Hence $z \equiv b \pmod{a}$.

(iii) $x + y = 2rs + s^2 - r^2$

$$= 2(t + k\frac{a}{2})(t + (k+1)\frac{a}{2}) + (t + (k+1)\frac{a}{2})^2 - (t + k\frac{a}{2})^2$$

$$= 2t^2 + 2tka + 2ta + k \frac{a}{2} a + ka^2 + \frac{a^2}{4}$$

$$\equiv 2t^2 + \frac{a^2}{4} \pmod{a}.$$

But $t \equiv \frac{2b+a}{4} \pmod{a}$. It follows that

$$x + y \equiv b + \frac{a}{2} + \frac{a^2}{4} \equiv b + \frac{a}{2}(1 + \frac{a}{2}) \pmod{a}.$$

Since $\frac{a}{2}$ is odd, then $1 + \frac{a}{2}$ is even. Hence $x + y \equiv b \pmod{a}$, which completes the proof.

Example 5. Let $a = 6$. Then $b = 1$ or 5. The set of quadratic residues (mod 6) is

$$Q = \{1,3,4\} .$$

If $b = 1$, since $1 \in Q$, then there exists t, say $t = 1$, such that $t^2 \equiv 1 \pmod{6}$. Let $r = a = 6$, $s = t + ka = 1 + 3.6 = 19$ (here, $k = 3$). Then

$$x = s^2 - r^2 = 325, \quad y = 2rs = 228, \quad z = s^2 + r^2 = 397,$$

which implies that $x - y = 97$, $x + y = 553$. Hence

$$6n_1 + 1 = x - y = 97$$

$$6n_2 + 1 = z = 397$$

$$6n_3 + 1 = x + y = 553 .$$

Whence $n_1 = 16$, $n_2 = 66$, $n_3 = 92$ and

$$(97)^2 + (553)^2 = 315218 = 2(397)^2 .$$

It follows that $(97)^2$, $(397)^2$, $(553)^2$ is a primitive 3-term arithmetic progression in $\{(6n+1)^2\}$.

If $b = 5$, since $\frac{2b+a}{4} = \frac{2.5+6}{4} = 4 \in Q$, then there exists t, say $t = 2$, such that $t^2 \equiv 4 \pmod{6}$. Let

$$r = t + k\frac{a}{2} = 2 + 1.3 = 5 ,$$

$$s = t + (k+1)\frac{a}{2} = 2 + 2.3 = 8$$

(here, $k = 1$). Then

$$x = 2rs = 80 , \quad y = s^2 - r^2 = 39 , \quad z = s^2 + r^2 = 89$$

which implies that $x-y = 41$, $x+y = 119$. Hence

$$6n_1 + 5 = x-y = 41$$

$$6n_2 + 5 = z = 89$$

$$6n_3 + 5 = x+y = 119 .$$

Whence $n_1 = 6$, $n_2 = 14$, $n_3 = 19$. Thus, $(41)^2$, $(89)^2$, $(119)^2$ is a primitive 3-term arithmetic progression in $\{(6n+5)^2\}$.

Example 6. Let $a = 22$. Then b is one of $1,3,5,7,9,13,15,17,19,21$. The set of quadratic residues (mod 22) is

$$Q = \{1,3,4,5,9,11,12,14,15,16,20\}.$$

For $b = 1,3,5,9,15$, we have $b \in Q$ and so $(a,b) \in T$.

For $b = 7,13,17,19,21$, we have $\frac{2b+22}{4} \in Q$ and again $(a,b) \in T$.

For example, if $b = 3$, there exists t , say $t = 5$, such that $t^2 \equiv 3 \pmod{22}$. Let $r = a = 22$, $s = t + ka = 5 + 3.22 = 71$ (here, $k = 3$). Then

$$x = s^2 - r^2 = (71)^2 - (22)^2 = 4557$$

$$y = 2rs = 2.22.71 = 3124$$

$$z = s^2 + r^2 = (71)^2 + (22)^2 = 5525$$

which implies that $x-y = 1433$ and $x+y = 7681$. Hence

$$22n_1 + 3 = x-y = 1433$$

$$22n_2 + 3 = z = 5525$$

$$22n_3 + 3 = x+y = 7681 .$$

Thus, $n_1 = 65$, $n_2 = 251$, $n_3 = 349$ and

$$(1433)^2 + 7681)^2 = 61051250 = 2(5525)^2 .$$

If $b = 13$, since $\frac{2.13 + 22}{4} = 12 \in Q$, then there exists t, say $t = 10$, such that $t^2 \equiv 12 \pmod{22}$. Let

$$r = t + k\frac{a}{2} = 10 + 1.11 = 21 ,$$

$$s = t + (k+1)\frac{a}{2} = 10 + 2.11 = 32 ,$$

(here, $k = 1$). Then

$$x = 2rs = 2.21.32 = 1344$$

$$y = s^2 - r^2 = (32)^2 - (21)^2 = 583$$

$$z = s^2 + r^2 = (32)^2 + (21)^2 = 1465$$

which implies that $x-y = 761$ and $x+y = 1927$. Hence

$$22n_1 + 13 = x-y = 761$$

$$22n_2 + 13 = z = 1465$$

$$22n_3 + 13 = x+y = 1927 .$$

Thus, $n_1 = 34$, $n_2 = 66$, $n_3 = 87$ and

$$(761)^2 + (1927)^2 = 4292450 = 2(1465)^2 .$$

Lemma 3.19. Let a be even such that $\frac{a}{2}$ is odd. Then the set of quadratic residues mod $\frac{a}{2}$ is contained in the set of quadratic residues mod a .

Proof. Let q be a quadratic residue mod $\frac{a}{2}$. Then there exists a positive integer t such that $t^2 \equiv q \pmod{\frac{a}{2}}$, i.e., $t^2 = q + k\frac{a}{2}$ for some integer k .

(i) If k is even, say $k = 2k_1$, then $t^2 = q + k_1$ and so $t^2 \equiv q \pmod{a}$. Hence q is quadratic residue mod a .

(ii) If k is odd, then let $t_1 = t + \frac{a}{2}$. Then $t_1^2 = (t + \frac{a}{2})^2 = t^2 + ta + \frac{a^2}{4} = q + k\frac{a}{2} + ta + \frac{a^2}{4} \equiv q + (k + \frac{a}{2})\frac{a}{2} \equiv q \pmod{a}$ since $k + \frac{a}{2}$ is even. Hence q is a quadratic residue mod a .

Theorem 3.20. Let a be even such that $\frac{a}{2}$ is odd. Let b be such that $a > b > 0$, $(a,b) = 1$. If $(a,b) \in T$, then b or $\frac{b + \frac{a}{2}}{2} = \frac{2b + a}{4}$ is a quadratic residue mod a.

Proof. Let $(a,b) \in T$. Then there exist $0 \leq n_1 < n_2 < n_3$ such that $(an_1 + b)^2$, $(an_2 + b)^2$, $(an_3 + b)^2$ is a primitive 3-term arithmetic progression in I^2. By virtue of Theorem 3.10, we have

$$an_1 + b = x-y, \quad an_2 + b = z, \quad an_3 + b = x+y,$$

where $x = \max\{2rs, s^2-r^2\}$, $y = \min\{2rs, s^2-r^2\}$, $z = s^2+r^2$, $s > r > 0$, $(r,s) = 1$ and r and s are of opposite parity. Hence

$$x-y \equiv z \equiv x+y \equiv b \pmod{a}.$$

It follows that

$$2x \equiv 2b \pmod{a}, \quad z \equiv b \pmod{a}, \quad 2y \equiv 0 \pmod{a}.$$

We consider two cases:

Case I. $x = x^2 + r^2$, $y = 2rs$, $z = s^2 + r^2$. It follows that

$$2(s^2 - r^2) \equiv 2b \pmod{a}, \quad s^2 + r^2 \equiv b \pmod{a}.$$

Hence $4s^2 \equiv 4b \pmod{a}$ which implies that $s^2 \equiv b \pmod{\frac{a}{2}}$ and so b is a quadratic residue mod $\frac{a}{2}$. By Lemma 3.19 b is a quadratic residue mod a.

Case II. $x = 2rs$, $y = s^2 - r^2$, $z = s^2 + r^2$. It follows that

$$2(s^2 - r^2) \equiv 0 \pmod{a}, \quad s^2 + r^2 \equiv b \pmod{a}.$$

Hence $4s^2 \equiv 2b \pmod{a}$ which implies that $2s^2 \equiv b \pmod{\frac{a}{2}}$ and so $s^2 \equiv \frac{b + \frac{a}{2}}{2} \equiv \frac{2b + a}{4} \pmod{\frac{a}{2}}$ since b, $\frac{a}{2}$ are odd. Hence $\frac{2b + a}{a}$ is a quadratic residue mod $\frac{a}{2}$. By virtue of Lemma 3.19, $\frac{2b + a}{4}$ is a quadratic residue mod a.

Theorem 3.21. Let $a = 2^n$, $n \geq 4$. Let b be such that $a > b > 0$, $(a,b) = 1$. Then $(a,b) \in T$ if and only if b is a quadratic residue mod a.

Proof. If b is a quadratic residue mod a, then, by the Theorem 3.17, $(a,b) \in T$.

Suppose $(a,b) \in T$. Then $(an_1+b)^2$, $(an_2+b)^2$, $(an_3+b)^2$ is a primitive 3-term arithmetic progression for some $0 \leq n_1 < n_2 < n_3$. By virtue of Theorem 3.10, we have

$$an_1 + b = x-y$$

$$an_2 + b = z \qquad (8)$$

$$an_3 + b = x+y$$

where $x = \max\{2rs, s^2-r^2\}$, $y = \min\{2rs, s^2-r^2\}$, $z = s^2 + r^2$, $s > r > 0$, $(r,s) = 1$ and r and s are of opposite parity. Equations (8) mean that $x-y \equiv z \equiv z+y \equiv b \pmod a$. It follows that

$$2x \equiv 2b \pmod a$$

$$z \equiv b \pmod a$$

$$2y \equiv 0 \pmod a .$$

We consider two cases:

Case I. $2rs > s^2-r^2$. Then $x = 2rs$, $y = s^2 - r^2$, $z = s^2 + r^2$. Hence we have $4rs \equiv 2b \pmod a$ which means that $a \mid 4rs - 2b$. That is, $2^{n-1} \mid 2rs - b$ which is impossible since $2rs - b$ is odd and $n \geq 4$. Hence we must have:

Case II. $s^2 - r^2 > 2rs$. Then $x = s^2 - r^2$, $y = 2rs$, $z = s^2 + r^2$. It follows that

$$2(s^2 - r^2) \equiv 2b \pmod a$$

$$s^2 + r^2 \equiv b \pmod a$$

$$4rs \equiv 0 \pmod a .$$

Since one of the r and s is even, say r even, then it follows, from $4rs \equiv 0 \pmod{a}$, that $2^{n-2} \mid r$. Hence $2^{2(n-2)} \mid r^2$. Whence, since $2(n-2) \geq n$, $2^n \mid r^2$. Therefore $r^2 \equiv 0 \pmod{a}$. Thus, $s^2 \equiv b \pmod{a}$ and b is a quadratic residue modulo a. Similarly if s is even.

Theorem 3.22. Let a be even such that $\frac{a}{2}$ is even, let b be such that $a > b > 0$, $(a,b) = 1$. If $b \equiv 3 \pmod{4}$, then $(a,b) \notin T$.

Proof. Suppose, on the contrary, that $(a,b) \in T$. Then $(an_1+b)^2$, $(an_2+b)^2$, $(an_3+b)^2$ is a primitive 3-term arithmetic progression for some n_1, n_2, n_3. It follows from Theorem 3.10 that

$$an_1 + b = x-y, \quad an_2 + b = z, \quad an_3 + b = x+y,$$

where, in particular, $z = s^2 + r^2$ and r and s are of opposite parity. Since $4 \mid a$, it follows that $z \equiv b \pmod{4}$ and so $s^2 + r^2 \equiv b \pmod{4}$. Since r and s are of opposite parity, $s^2 + r^2 \equiv 1 \pmod{4}$. Hence $b \equiv 1 \pmod{4}$ a contradiction since $b \equiv 3 \pmod{4}$.

Example 7. Let $a = 4$. Then $b = 1$ or 3. Since 1 is a quadratic residue mod 4, then, by Theorem 3.17, $(4,1) \in T$. Since $3 \equiv 3 \pmod{4}$, then, by Theorem 3.22, $(4,3) \notin T$.

Example 8. Let $a = 8$. Then b is one of $1,3,5,7$. The set of quadratic residue (mod 8) is

$$Q = \{0,1,4\}.$$

If $b = 1$, then $b \in Q$. Hence, by Theorem 3.17, $(8,1) \in T$. If $b = 3$ or 7, then $b \equiv 3 \pmod 4$. Hence, by Theorem 3.22, $(8,3) \notin T$ and $(8,7) \notin T$.

Finally, $b = 5$. None of our theorems handle this case. However, we can prove $(8,5) \notin T$ as follows:

Assume $(8,5) \in T$. As in the proof of Theorem 3.20 we can get

$$2x \equiv 2.5 \equiv 2 \pmod 8, \quad z \equiv 5 \pmod 8, \quad 2y \equiv 0 \pmod 8.$$

We have to consider two cases:

Case I. $x = 2rs$, $y = s^2 - r^2$, $z = s^2 + r^2$. This case implies that $8 \mid 4rs - 2$, i.e., $4 \mid 2rs - 1$ which is impossible since $2rs - 1$ is odd.

Case II. $x = s^2 - r^2$, $y = 2rs$, $z = s^2 + r^2$. It follows that

$$2(s^2 - r^2) \equiv 2 \pmod 8, \; s^2 + r^2 \equiv 5 \pmod 8, \quad 4rs \equiv 0 \pmod 8.$$

From $s^2 + r^2 \equiv 5 \pmod 8$, we have either

$$s^2 \equiv 1 \pmod 8 \quad \text{and} \quad r^2 \equiv 4 \pmod 8$$

or

$$s^2 \equiv 4 \pmod 8 \quad \text{and} \quad r^2 \equiv 1 \pmod 8.$$

But, since $2(s^2 - r^2) \equiv 2 \pmod 8$, then we must have

$$s^2 \equiv 1 \pmod 8 \quad \text{and} \quad r^2 \equiv 4 \pmod 8 .$$

This means that $s \equiv 1,3,5$ or $7 \pmod 8$ and $r \equiv 2$ or $6 \pmod 8$. It follows that $2rs \equiv 4 \pmod 8$. Hence

$$x-y = s^2 - r^2 - 2rs \equiv 1-4-4 \equiv 1 \pmod 8.$$

Therefore, there is no n such that $x-y = 8n + 5$. Thus $(8,5) \notin T$.

Finally, we remark that we are told by Professor Tom Brown from Dr. R. Graham of Bell Labs, there are no 4-term arithmetic progressions in I^2 (although we have never been shown a proof.) This implies that $f(n) = \alpha n^2 + \beta n + \gamma$, for $\alpha > 0$, does not contain any 4-term arithmetic progression.

BIBLIOGRAPHY

[1] Brown, T.C. and Freedman, A.R., Arithmetic Progressions in Lacunary sets. To appear in Rocky Mountain J. Math.

[2] Abramowitz, Milton and Stegun, Irene A., Editors, Handbook of Mathematical Functions. Dover Publications, Inc., New York, 1972.

[3] Fraleigh, John B., A First Course in Abstract Algebra, Third Edition, Addison-Wesley Publishing Company, Inc., 1982.

[4] Gioia, Anthony A., The Theory of Numbers, Markham Publishing Company, 1970.