PRIMITIVE PYTHAGOREAN TRIPLES WITH SUM OR DIFFERENCE OF LEGS EQUAL TO A PRIME*

DELANO P. WEGENER
Central Michigan University, Mt. Pleasant, Michigan 48858

1. INTRODUCTION

A pythagorean triple is a triple of natural numbers (x,y,z) such that $x^2 + y^2 = z^2$. Such a triple is called a primitive pythagorean triple if the components are relatively prime in pairs. It is well known [5, pp. 4–6] that all primitive pythagorean triples are given, without duplication, by:

$$x = 2mn, \qquad y = m^2 - n^2, \qquad z = m^2 + n^2 . \tag{1.1}$$

where m and n are relatively prime natural numbers which are of opposite parity and satisfy $m > n$. Conversely, if m and n $(m > n)$ are relatively prime natural numbers of opposite parity, then they generate a primitive pythagorean triple according to (1.1).

In this paper I will adhere to the following conventions:

(a) The first entry of a pythagorean triple will be the even leg of the triple.
(b) The second entry of a pythagorean triple will be the odd leg of the triple.
(c) The third entry of a pythagorean triple will be the hypotenuse and will never be called a leg of the triple.
(d) The natural numbers m and n in Eq. (1.1) will be called the generators of the triple (x,y,z).

Since every prime of the form $4k + 1$ can be written as the sum of two relatively prime natural numbers [6, p. 351] it follows that there are infinitely many primitive pythagorean triples with the hypotenuse equal to a prime. It is also easy to see that there are infinitely many primitive pythagorean triples with the odd leg equal to a prime, by noting that for any odd prime p, $m = (p + 1)/2$ and $n = (p - 1)/2$ generate a primitive pythagorean triple with the odd leg equal to p. It is completely trivial to show that the even leg is never a prime. Thus it is an easy problem to determine whether there are an infinite number of primitive pythagorean triples with any one of its components equal to a prime. However, the problem changes drastically if we try to determine whether there are an infinite number of primitive pythagorean triples with more than one component or some linear combination of the components equal to a prime. For example Waclaw Sierpinski [5, p. 6], [7, p. 94] raised the following question:

SIERPINSKI'S PROBLEM: Are there an infinite number of primitive pythagorean triples with both the hypotenuse and the odd leg equal to a prime?

This problem is equivalent to asking for an infinite number of solutions, in primes, to the Diophantine equation $q^2 = 2p - 1$. This equivalence is easily proved by noting that if (t,q,p) is a primitive pythagorean triple with p and q both prime, then

$$q^2 = p^2 - t^2 = (p - t)(p + t).$$

Since q is prime and $p + t > p - t > 0$, it follows that $q^2 = p + t$ and $p - t = 1$. Hence $q^2 = 2p - 1$. Conversely, if $q^2 = 2p - 1$, then $(p - 1, q, p)$ is a primitive pythagorean triple. Other than this simple transformation, it seems that no progress has been made toward a solution to Sierpinski's problem.

As a result of his involvement with Sierpinski's Problem, Professor I.A. Barnett was quite naturally led to the following similar questions.

*The research for this paper was supported in part by Ohio University Research Grant number OUR 252.

QUESTION A: Are there an infinite number of primitive pythagorean triples for which the sum of the legs is a prime?

QUESTION B: Are there an infinite number of primitive pythagorean triples for which the absolute value of the difference of the legs is a prime?

QUESTION C: Are there an infinite number of primitive pythagorean triples for which both the sum of the legs and the absolute value of the difference of the legs are prime?

Questions A and B are both answered in the affirmative [8]. In this paper we present a complete characterization of those triples which have either the sum or the difference of the legs equal to a prime. Question C is much more difficult and is discussed in some detail in this author's Ph.D. dissertation. The results related to Question C will be the subject of a future paper.

A few basic facts about the integral domain

$$Z[\sqrt{2}] = \left\{ a + b\sqrt{2} \mid a, b \in Z \right\}$$

and about the Pell equation $u^2 - 2v^2 = p$, where p is a prime, will facilitate the discussion of Questions A and B. The facts about the integral domain $Z[\sqrt{2}]$ will simply be stated with references to the proofs. However, the discussion of $u^2 - 2v^2 = p$ in Section 3 will be more detailed because it is quite elementary and is significantly different from the usual discussions of this particular Pell equation.

2. THE INTEGRAL DOMAIN $Z[\sqrt{2}]$

For the remainder of this article, I will follow the usual custom of referring to elements of $Z[\sqrt{2}]$ as integers and elements of Z as rational integers and I will use the following notation:

If

$$\alpha = a + b\sqrt{2},$$

then

$$\bar{\alpha} = a - b\sqrt{2}$$

is called the conjugate of α.

$$N(\alpha) = \alpha\bar{\alpha}$$

is called the norm of α.

$$R(\alpha) = a$$

is called the rational part of α.

$$I(\alpha) = b$$

is called the irrational part of α.

$$\epsilon = 1 + \sqrt{2}$$

is called the fundamental unit in $Z[\sqrt{2}]$.

$$\epsilon^{-1} = -1 + \sqrt{2}$$

is called the inverse of ϵ.

As usual, a unit of $Z[\sqrt{2}]$ is defined to be a non-zero element of $Z[\sqrt{2}]$ which has an inverse in $Z[\sqrt{2}]$, or equivalently, an element of $Z[\sqrt{2}]$ whose norm is ± 1. The set of units of $Z[\sqrt{2}]$ is precisely the set of

$$\left\{ \pm\epsilon^n \mid n \in Z \right\}$$

[4, p. 235], [2, p. 209] and for this reason ϵ is called the fundamental unit of $Z[\sqrt{2}]$.

If α and δ are integers and there is a unit γ such that $\alpha = \delta\gamma$, then α is called an associate of δ. A non-zero element of $Z[\sqrt{2}]$, which is not a unit, is a prime if and only if it is divisible only by units and associates of itself. It is easily shown that if α and δ are associates, then

$$N(\alpha) = \pm N(\delta),$$

but the converse is in general not true. However, if α and δ are both primes and $N(\alpha) = \pm N(\delta)$, then α is an associate of either δ or $\bar{\delta}$. The primes of $Z[\sqrt{2}]$ are all associates of:

(1) $\sqrt{2}$

(2) All rational primes of the form $8k \pm 3$. These are frequently called prime of the second degree.

(3) All conjugate factors of rational primes of the form $8k \pm 1$. These are frequently called primes of the first degree. This result is found in any discussion of the integral domain $Z[\sqrt{2}]$, for example [4, p. 240], [2, p. 221].

Each of the properties, listed below, in Lemma 2.1, is an elementary consequence of the definitions of the symbols involved. Consequently, they are listed without proof.

Lemma 2.1: If α and β are integers, then

$$\alpha + \bar{\alpha} = 2R(\alpha)$$

$$\alpha - \bar{\alpha} = 2\sqrt{2}I(\alpha)$$

$$R(\alpha\beta) = R(\alpha)R(\beta) + 2I(\alpha)I(\beta)$$

$$I(\alpha\beta) = I(\alpha)R(\beta) + R(\alpha)I(\beta)$$

$$R(\alpha\bar{\beta}) = R(\alpha)R(\beta) - 2I(\alpha)I(\beta)$$

$$I(\alpha\bar{\beta}) = R(\beta)I(\alpha) - R(\alpha)I(\beta)$$

$$R(\alpha\varepsilon) = R(\alpha) + 2I(\alpha)$$

$$I(\alpha\varepsilon) = R(\alpha) + I(\alpha)$$

3. THE PELL-TYPE EQUATION $u^2 - 2v^2 = p$

Most number theory books have some discussion of the Pell equation and Pell-type equations. A particularly good discussion is to be found in Chapter VI of [3] and a very detailed history is found in Chapter XII of [1]. In this paper we only need consider the very special Pell-type equation

$$u^2 - 2v^2 = p, \tag{3.1}$$

where p is a rational prime.

As usual, any two rational integers $u = a$, $v = b$ will be called a solution of Eq. (3.1) if $a^2 - 2b^2 = p$. It follows from the previous section that $u = a$, $v = b$ is a solution if and only if

$$N(a + b\sqrt{2}) = p.$$

From the discussion of primes in $Z[\sqrt{2}]$, it is clear that Eq. (3.1) has a solution if and only if the rational prime p is of the form $8k \pm 1$.

If

$$N(a + b\sqrt{2}) = p,$$

then the four solutions

$$u = a, \quad v = b; \qquad u = a, \quad v = -b; \qquad u = -a, \quad v = b; \qquad u = -a, \quad v = -b$$

are said to be the solutions obtained from $a + b\sqrt{2}$. Notice that the same four solutions are obtained from each of

$$a + b\sqrt{2}, \qquad \overline{a + b\sqrt{2}}, \qquad -(a + b\sqrt{2}) \quad \text{and} \quad \overline{-(a + b\sqrt{2}}.$$

It is easily shown [4, p. 242] that if $\alpha = a + b\sqrt{2}$ and $N(\alpha) = p$, then all solutions of Eq. (1.2) are obtained from

$$\{\alpha\varepsilon^{2t} \mid t \in Z\}$$

and conversely, every element of

$$\{\alpha\varepsilon^{2t} \mid t \in Z\}$$

yields a solution of Eq. (3.1).

The equation

$$u^2 - 2v^2 = p$$

may easily be transformed to the equation

$$\frac{u^2}{(\sqrt{p})^2} - \frac{v^2}{(\sqrt{p/2})^2} = 1,$$

which is the standard equation of a hyperbola. Thus integer solutions of Eq. (3.1) are easily associated with lattice points on the above hyperbola. Figure 1 is a graph of this hyperbola. Reference to Fig. 1 makes it clear that if $u = a > 0$ and $v = b > 0$ is a solution of Eq. (3.1), and then

$$\sqrt{p} < a < \sqrt{2p} \qquad \text{and} \qquad 0 < b < \sqrt{p/2}$$

are equivalent. The remainder of this section will show that there is exactly one solution which satisfies these conditions.

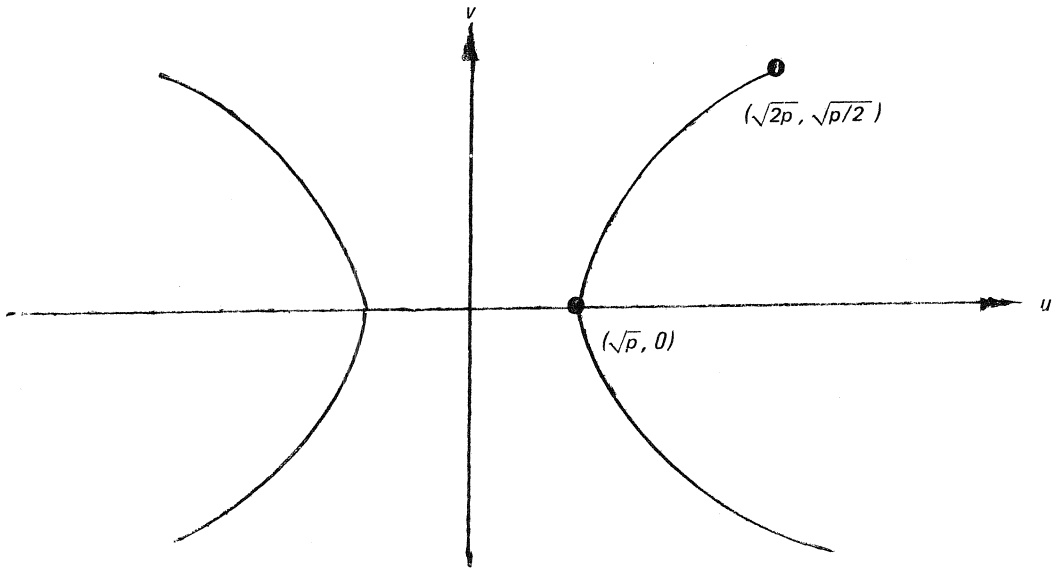

Figure 1

If p is a rational prime of the form $8k \pm 1$, then the set

$$S = \left\{ (u,v) \mid u \in Z, v \in Z, u > 0, v > 0, u^2 - 2v^2 = p \right\}$$

is infinite and contains an element (a,b) with minimal first component. Since

$$(a + b\sqrt{2})\epsilon^{-2} = (3a - 4b) + (3b - 2a)\sqrt{2}$$

it follows that

$$u = 3a - 4b \qquad \text{and} \qquad v = 3b - 2a$$

satisfy

$$u^2 - 2v^2 = p.$$

Note that

$$a^2 - 2b^2 = p > 0$$

implies that $b < a/\sqrt{2}$. Thus

$$3a - 4b > 3a - 4a\sqrt{2} = a(3 - 2\sqrt{2}) > 0.$$

Hence either

$$(3a - 4b, 3b - 2a) \quad \text{or} \quad (3a - 4b, 2a - 3b)$$

is in S. In either case we have

$$a \leqslant 3a - 4b,$$

which implies that

$$4b^2 \leqslant a^2 = p + 2b^2,$$

and this in turn implies that $b < \sqrt{p/2}$. Hence there is at least one solution $u = a$, $v = b$ of $u^2 - 2v^2 = p$ with

$$\sqrt{p} < a < \sqrt{2p} \quad \text{and} \quad 0 < b < \sqrt{p/2}.$$

To show that there is only one solution of (3.1) which satisfies the above inequalities it is helpful to observe that: For every $\beta \in Z[\sqrt{2}]$,

$$R(\beta\epsilon^2) = 3R(\beta) + 4I(\beta)$$
$$I(\beta\epsilon^2) = 2R(\beta) + 3I(\beta)$$
$$R(\beta\epsilon^{-2}) = 3R(\beta) - 4I(\beta)$$
$$I(\beta\epsilon^{-2}) = 3I(\beta) - 2R(\beta).$$

It follows from these equalities that if $R(\beta) > 0$ and $I(\beta) > 0$, then

$$R(\beta\epsilon^{-2}) < R(\beta\epsilon^2) \quad \text{and} \quad R(\beta\epsilon^{2t}) < R(\beta\epsilon^{2t+2})$$

for all $t \geqslant 0$. Note also that if $R(\beta) > 0$, then $I(\beta) < 0$ implies that

$$R(\beta\epsilon^{-2t}) < R(\beta\epsilon^{-2t-2})$$

for all $t > 0$.

Let $\alpha = a + b\sqrt{2}$ with

$$\sqrt{p} < a < \sqrt{2p} \quad \text{and} \quad 0 < b < \sqrt{p/2}$$

and let $u = a$, $v = b$ be a solution of (3.1). Then

$$\alpha\epsilon^2 = (3a + 4b) + (2a + 3b)\sqrt{2}$$

and

$$\alpha\epsilon^{-2} = (3a - 4b) + (3b - 2a)\sqrt{2}.$$

Clearly

$$3a - 4b < 3a + 4b$$

and from the previous remarks it follows that the rational parts of $\alpha\epsilon^{2t}$, $t \geqslant 0$, form a strictly increasing sequence. If we assume that $3b - 2a \geqslant 0$, then $9b^2 \geqslant 4a^2$ and hence

$$-4p + b^2 = -4(a^2 - 2b^2) + b^2 \geqslant 0.$$

But then $b^2 \geqslant 4p$ and

$$b \geqslant 2\sqrt{p} > (1/\sqrt{2})\sqrt{p} = \sqrt{p/2}.$$

This contradiction shows that $3b - 2a < 0$ and from the previous remarks it follows that the rational parts of $\alpha\epsilon^{-2t}$, $t \geq 1$, form an increasing sequence.

If we assume $3a - 4b \leq a$, then $a^2 \leq 4b^2$ and hence

$$p - 2b^2 = a^2 - 2b^2 - 2b^2 = a^2 - 4b^2 \leq 0.$$

But then $\sqrt{p/2} \leq b$ and we conclude that

$$3a - 4b > a > \sqrt{p} > 0.$$

It now follows that if

$$3a - 4b > \sqrt{2p},$$

then the rational part of $\alpha\epsilon^{2t}$ will be greater than $\sqrt{2p}$ for all $t \neq 0$.

If we assume

$$3a - 4b \leq \sqrt{2p},$$

then by squaring both sides and collecting terms we have

$$17a^2 - 10p \leq 24a\sqrt{(a^2 - p)/2}.$$

Note that

$$17a^2 - 10p = 7a^2 + 20b^2 > 0.$$

Squaring both sides again and simplifying yields

$$a^4 - 52a^2p + 100p^2 \leq 0,$$

which can be written as

$$(a^2 - 10p)^2 \leq 32a^2p.$$

This is a contradiction because

$$a^2 - 10p < 2p - 10p = -8p$$

and hence

$$(a^2 - 10p)^2 > 64p^2 = (32p)(2p) > 32pa^2.$$

Thus

$$3a - 4b > \sqrt{2p}.$$

This establishes that there is at most one solution $u = a$, $v = b$ such that $\sqrt{p} < a < \sqrt{2p}$.

The material in this section is summarized in Lemma 3.2 below:

Lemma 3.2. If p is a rational prime of the form $8k \pm 1$, the equation $u^2 - 2v^2 = p$ has exactly one solution $u = a$, $v = b$ such that the following two equivalent statements are true:

(i) $$\sqrt{p} < a < \sqrt{2p}$$

(ii) $$0 < b < \sqrt{p/2}.$$

The equation $u^2 - 2v^2 = p$ has infinitely many solutions, all of which are obtained from

$$(a + b\sqrt{2})\epsilon^{2t},$$

where t is any rational integer and $u = a$, $v = b$ is any solution of $u^2 - 2v^2 = p$.

The unique solution which satisfies (i) and (ii) will be called the *fundamental solution* of $u^2 - 2v^2 = p$.

4. PRIMITIVE PYTHAGOREAN TRIPLES WITH SUM OF LEGS EQUAL TO A PRIME

The theorems of this section show that if (x,y,z) is a primitive pythagorean triple with $x + y$ equal to a prime p, then p is of the form $8k \pm 1$, and conversely, if p is a prime of the form $8k \pm 1$, then there is a unique primitive pythagorean triple (x,y,z) such that $x + y = p$. Since there are infinitely many primes of the form $8k \pm 1$, this yields an affirmative answer to Question A of Section 1.

Theorem 4.1. If (x,y,z) is a primitive pythagorean triple and p is a prime divisor of $x + y$ or $|x - y|$, then p is of the form $8k \pm 1$.

Proof. Suppose p divides $x + y$ or $|x - y|$. Note this implies $(x,p) = (y,p) = 1$, and $x \equiv \pm y \pmod{p}$ so that

$$2x^2 \equiv x^2 + y^2 \equiv z^2 \pmod{p}. \tag{1}$$

By definition, x^2 is a quadratic residue of p. The congruence (1) implies $2x^2$ is also a quadratic residue of p. If p were of the form $8k \pm 3$, then 2 would be a quadratic nonresidue of p [3, pp. 136–139] and since x^2 is a quadratic residue of p, $2x^2$ would be a quadratic nonresidue of p, contradicting (1). Thus p must be of the form $8k \pm 1$.

Corollary. If x and y are the legs of a primitive pythagorean triple, then both $x + y$ and $|x - y|$ are of the form $8k \pm 1$.

This corollary is immediate from the theorem but it should be pointed out that the corollary may be proved directly by considering the following two cases:

$$m = 2r, \quad n = 2t + 1$$

$$m = 2r, + 1, \quad n = 2t,$$

where m and n are the generators of the primitive pythagorean triple.

Theorem 4.2. For every prime p of the form $8k \pm 1$ there exists a primitive pythagorean triple (x,y,z) such that $x + y = p$.

Proof. Let p be a prime of the form $8k \pm 1$ and let $u = a$, $v = b$ be the fundamental solution of $u^2 - 2v^2 = p$. Let $m = a - b$ and $n = b$. Note $(m,n) = 1$ because $(a,b) = 1$. Clearly m and n are of opposite parity because $m + n = a \equiv 1 \pmod 2$. If $m \leqslant n = b$, then

$$p + 2b^2 = a^2 = (n + m)^2 \leqslant 4b^2$$

and thus $b \geqslant p/2$, a contradiction. Hence $m > n$. Thus m and n generate the primitive pythagorean triple

$$x = 2mn, \qquad y = m^2 - n^2, \qquad z = m^2 + n^2 .$$

For this triple

$$x + y = 2mn + m^2 - n^2 = (m + n)^2 - 2n^2 = a^2 - 2b^2 = p.$$

Theorem 4.3. If p is a prime of the form $8k \pm 1$, then there is exactly one primitive pythagorean triple (x,y,z) such that $x + y = p$.

Proof. Let m and n generate a primitive pythagorean triple (x,y,z) such that $x + y = p$. Then

$$(m + n)^2 - 2n^2 = p.$$

Since $m > n$ it follows that

$$p = (m+n)^2 - 2n^2 > (2n)^2 - 2n^2 = 2n^2,$$

which implies that $n < \sqrt{p/2}$. Thus $u = m + n$, $v = n$ is the fundamental solution of $u^2 - 2v^2 = p$, and hence, by Lemma 3.2, m and n are uniquely determined.

5. PRIMITIVE PYTHAGOREAN TRIPLES WITH DIFFERENCE OF LEGS EQUAL TO A PRIME

The material in this section is related to Question B of Section 1. The first theorem provides an affirmative answer to Question B by showing that every prime of the form $8k \pm 1$ is equal to the difference of the legs of some primitive pythagorean triple. The second theorem shows that for every prime of the form $8k \pm 1$ there is an infinite number of primitive pythagorean triples with the difference of legs equal to that prime. W.P. Whitlock, Jr. [8] discusses briefly these same two theorems and points out that these methods were essentially known to Frenicle. The remainder of this section is devoted to the characterization of all primitive pythagorean triples with difference of legs equal to a prime.

Theorem 5.1. For every prime p of the form $8k \pm 1$ there is a primitive pythagorean triple (x,y,z) such that $|x - y| = p$.

Proof. Let p be any prime of the form $8k \pm 1$ and let $u = a$, $v = b$ be the fundamental solution of $u^2 - 2v^2 = p$. Then, as in Theorem 4.2, it is easily shown that $m = a + b$ and $n = b$ generate a primitive pythagorean triple (x,y,z) with $x - y = -p$.

If p is a prime of the form $8k \pm 1$, then, as pointed out in Section 4, there is a unique primitive pythagorean triple (x,y,z) such that $x + y = p$. The fact that there is no such uniqueness when discussing the difference of legs follows from the theorem below.

Theorem 5.2. If m,n $(m > n)$ generate a primitive pythagorean triple (x,y,z) then $M = 2m + n$ and $N = m$ generate a primitive pythagorean triple (X,Y,Z) such that $|X - Y| = |x - y|$.

The proof is computational and is left to the reader.

The previous two theorems make it easy to show that for each prime p of the form $8k \pm 1$ there is an infinite number of primitive pythagorean triples (x,y,z) such that $|x - y| = p$. This is done by defining an infinite sequence

$$\{T_j(p)\}$$

of primitive pythagorean triples (x_j,y_j,z_j) such that $|x_j - y_j| = p$ for all j.

Definition 1. Let p be a fixed prime of the form $8k \pm 1$ and let a and b be the unique natural numbers such that

$$a^2 - 2b^2 = p, \qquad \sqrt{p} < a < \sqrt{2p}, \quad \text{and} \quad 0 < b < \sqrt{p/2}.$$

Define the sequence $\{T_j(p)\}$ as follows:

Let $T_0(p)$ be the primitive pythagorean triple generated by $m_0 = a + b$ and $n = b$. For all $j \geq 1$, define $T_j(p)$ to be the primitive pythagorean triple generated by

$$m_j = 2m_{j-1} + n_{j-1}, \qquad \text{and} \qquad n_j = m_{j-1}.$$

Figures 2 and 3 illustrate the sequence $\{T_j(p)\}$.

An examination of a table of primitive pythagorean triples shows that for each prime p of the form $8k \pm 1$ there are primitive pythagorean triples (x,y,z) with $|x - y| = p$ which are not in $\{T_j(p)\}$. The next theorem will be used to show that for each prime p of the form $8k \pm 1$ there is in fact another infinite sequence $\{T'_j(p)\}$ of primitive

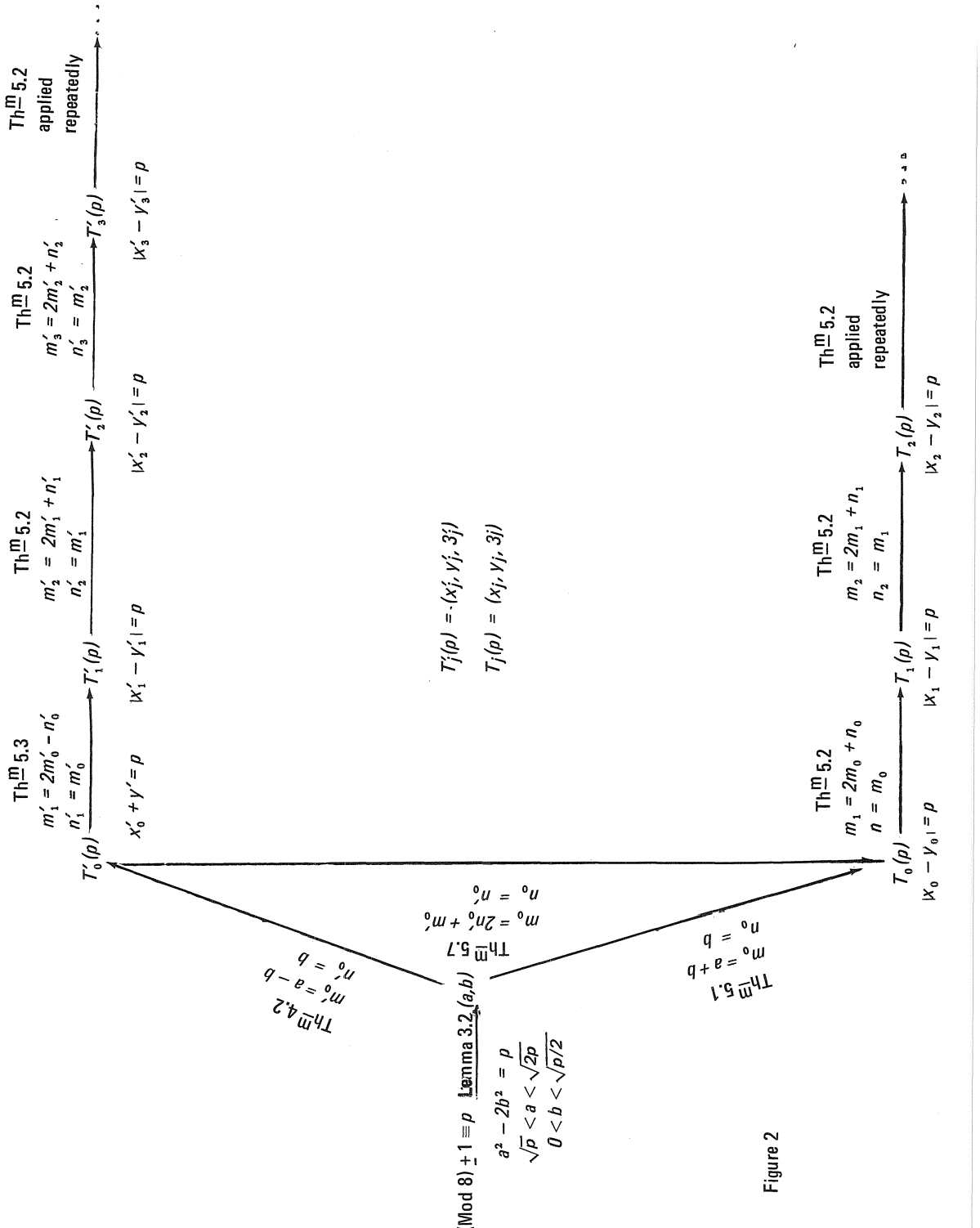
Th 5.2 applied repeatedly
Th 5.2
Th 5.3
Th 4.2
Th 5.7
Th 5.1
Lemma 3.2
(Mod 8) ±1 ≡ p
$a^2 - 2b^2 = p$
$\sqrt{p} < a < \sqrt{2p}$
$0 < b < \sqrt{p/2}$
$T_0(p)$
$T_1(p)$
$T_2(p)$
$T_3(p)$
$T'_0(p)$
$T'_1(p)$
$T'_2(p)$
$T'_3(p)$
$T_j(p) = (x_j, y_j, 3j)$
$T'_j(p) = (x'_j, y'_j, 3j)$
$m_0 = a + b$
$n_0 = b$
$m_0 = 2n'_0 + m'_0$
$n_0 = n'_0$
$m'_0 = a - b$
$n'_0 = b$

Figure 2

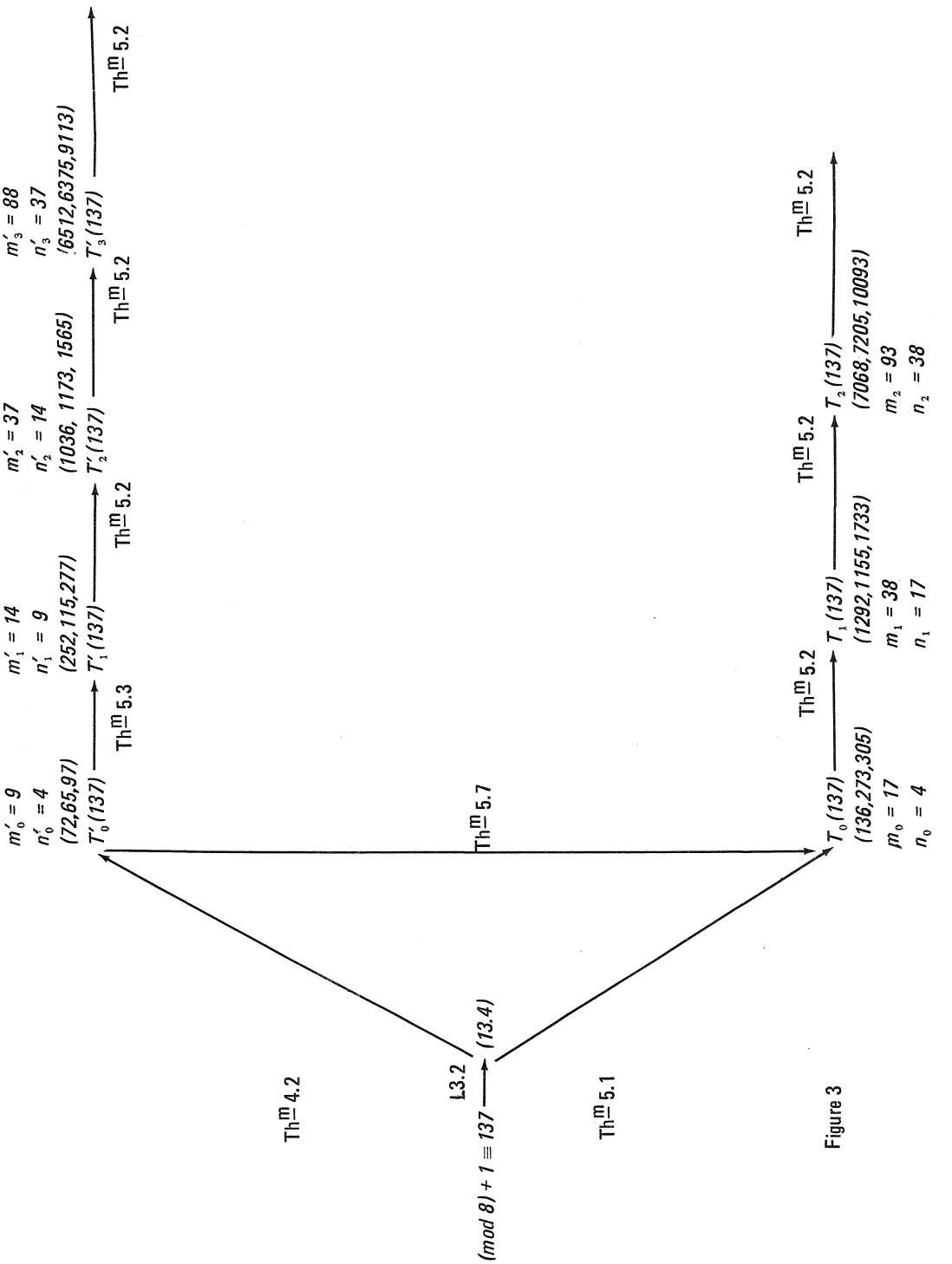
$m'_0 = 9$
$n'_0 = 4$
(72,65,97)
$T'_0(137)$
Th^{m} 5.3
$m'_1 = 14$
$n'_1 = 9$
(252,115,277)
$T'_1(137)$
Th^{m} 5.2
$m'_2 = 37$
$n'_2 = 14$
(1036, 1173, 1565)
$T'_2(137)$
Th^{m} 5.2
$m'_3 = 88$
$n'_3 = 37$
(6512,6375,9113)
$T'_3(137)$
Th^{m} 5.2
Th^{m} 5.7
Th^{m} 4.2
L3.2
(mod 8) + 1 ≡ 137
(13.4)
Th^{m} 5.1
Th^{m} 5.2
$T_0(137)$
(136,273,305)
$m_0 = 17$
$n_0 = 4$
Th^{m} 5.2
$T_1(137)$
(1292,1155,1733)
$m_1 = 38$
$n_1 = 17$
Th^{m} 5.2
$T_2(137)$
(7068,7205,10093)
$m_2 = 93$
$n_2 = 38$

Figure 3

pythagorean triples (x_j', y_j', z_j') such that

$$|x_j' - y_j'| = p$$

for $j \geq 1$ and

$$x_j' + y_j' = p$$

for $j = 0$.

Theorem 5.3. If m and n $(m > n)$ generate a primitive pythagorean triple (x,y,z), then $M = 2m - n$ and $N = m$ generate a primitive pythagorean triangle (X,Y,Z) such that $|X - Y| = x + y$.

The proof is computational and is left to the reader.

Definition 2. Let p, a and b be the same as in the construction to $\{T_j(p)\}$. Define the sequence $\{T_j'(p)\}$ as follows: Let $T_0'(p)$ be the triple generated by $m_0' = a - b$ and $n_0' = b$. Let $T_1'(p)$ be the triple generated by

$$m_1' = 2m_0' - n_0' \quad \text{and} \quad n_1' = m_0' .$$

For all $j \geq 2$, define $T_j'(p)$ to be the primitive pythagorean triple generated by

$$m_j' = 2m_{j-1}' + n_{j-1}' \quad \text{and} \quad n_j' = m_{j-1}' .$$

Figures 2 and 3 illustrate the sequence $\{T_j'(p)\}$

Theorem 5.4. Let p be a prime of the form $8k \pm 1$. If T is the set of triples

$$\{T_j(p) \mid j = 0, 1, 2, \cdots\}$$

and T' is the set of triples $\{T_j'(p) \mid j = 1, 2, \cdots\}$, then $T \cap T' = \phi$.

Proof. Suppose there is a $T_r(p)$ in T and a $T_s'(p)$ in T' such that $r \geq 1$, $s \geq 2$ and $T_r(p) = T_s'(p)$. Then $m_r = m_s'$ and $n_r = n_s'$ and hence

$$m_{r-1} = n_r = n_s' = m_{s-1}' ,$$

which in turn implies

$$2m_{s-1}' + n_{r-1} = 2m_{r-1} + n_{r-1} = m_r = m_s' = 2m_{s-1}' + n_{s-1}' ,$$

and thus $n_{r-1} = n_{s-1}'$. Hence

$$T_{r-1}(p) = T_{s-1}'(p) .$$

Repeating this argument a finite number of times results in one of the following cases:

Case 1. $T_0(p) = T_{s-r}'(p)$ if $s > r + 1$.

Case 2. $T_0(p) = T_1'(p)$ if $s = r + 1$.

Case 3. $T_{r-s}(p) = T_1'(p)$ if $s < r + 1$.

To complete the proof it suffices to show that each of these cases is impossible. In Case 1,

$$b = n_0 = n_{s-r}' = m_{s-r-1}' > n_{s-r-1}' = \cdots = m_0' > n_0' = b,$$

a contradiction. In Case 3,

$$m_{r-s-1} = n_{r-s} = n'_1 = m'_0$$

and

$$2m_{r-s-1} + n_{r-s-1} = m_{r-s} = m'_1 = 2m'_0 = n'_0.$$

Hence

$$0 < n_{r-s-1} = -n'_0 < 0$$

which is again a contradiction.

The above description of the sequences

$$\{T_j(p)\} \qquad \text{and} \qquad \{T'_j(p)\}$$

gives a convenient method for constructing a triple of the sequence from the preceding triple. It is also possible to give an explicit formula for a triple in the sequence in terms of the fundamental solution of $u^2 - 2v^2 = p$. Certain properties of the triples in the sequence become more accessible when viewed in this way. One such property is stated in Theorem 5.6.

Theorem 5.5. Let p be a prime of the form $8k \pm 1$. Let $u = a$, $v = b$ be the fundamental solution of

$$u^2 - 2v^2 = p$$

and let

$$\alpha = a + b\sqrt{2}.$$

(1) For $j \geq 0$, $T_j(p)$ is generated by:

$$m_j = R(\alpha\epsilon^j) + I(\alpha\epsilon^j) = I(\alpha\epsilon^{j+1})$$

$$n_j = I(\alpha\epsilon^j).$$

(2) For $j > 0$, $T'_j(p)$ is generated by:

$$m'_j = R(\bar{\alpha}\epsilon^j) + I(\bar{\alpha}\epsilon^j) = I(\bar{\alpha}\epsilon^{j+1})$$

$$n'_j = I(\bar{\alpha}\epsilon^j).$$

(3) For $j \geq 0$, $T_j(p)$ is generated by:

$$m_j = \frac{\epsilon^{j+1} - \bar{\epsilon}^{j+1}}{2\sqrt{2}}\, a + \frac{\epsilon^{j+1} + \bar{\epsilon}^{j+1}}{2}\, b$$

$$n_j = \frac{\epsilon^j - \bar{\epsilon}^j}{2\sqrt{2}}\, a + \frac{\epsilon^j + \bar{\epsilon}^j}{2}\, b.$$

(4) For $j > 0$, $T'_j(p)$ is generated by:

$$m'_j = \frac{\epsilon^{j+1} - \bar{\epsilon}^{j+1}}{2\sqrt{2}}\, a - \frac{\epsilon^{j+1} + \bar{\epsilon}^{j+1}}{2}\, b$$

$$n'_j = \frac{\epsilon^j - \bar{\epsilon}^j}{2\sqrt{2}}\, a - \frac{\epsilon^j + \bar{\epsilon}^j}{2}\, b.$$

Proof (of (1)). By construction, $T_0(p)$ is generated by

$$m_0 = a+b = R(a\epsilon^0)+I(a\epsilon^0)$$

and

$$n_0 = b = I(a\epsilon^0).$$

Make the induction hypothesis that $T_j(p)$ is generated by

$$m_j = R(a\epsilon^j)+I(a\epsilon^j) \quad \text{and} \quad n_j = I(a\epsilon^j).$$

Then by construction, $T_{j+1}(p)$ is generated by

$$m_{j+1} = 2R(a\epsilon^j)+3I(a\epsilon^j) \quad \text{and} \quad n_j = R(a\epsilon^j)+I(a\epsilon^j).$$

By Lemma 2.1,

$$R(a\epsilon^{j+1}) = R(a\epsilon^j)+2I(a\epsilon^j) \quad \text{and} \quad I(a\epsilon^{j+1}) = R(a\epsilon^j)+I(a\epsilon^j).$$

Now it is clear that

$$m_{j+1} = R(a\epsilon^{j+1})+I(a\epsilon^{j+1})+I(a\epsilon^{j+1})$$

and

$$n_{j+1} = I(a\epsilon^{j+1}).$$

It follows directly from Lemma 2.1, that

$$m_j = R(a\epsilon^j)+I(a\epsilon^j) = I(a\epsilon^{j+1}).$$

Thus the formulae in (1) hold for all $j \geqslant 0$. The formulae in (2) are proved in exactly the same way. The formulae in (3) are proved by using Lemma 2.1 to get

$$m_j = R(a\epsilon^j)+I(a\epsilon^j) = I(a\epsilon^{j+1}) = I(\epsilon^{j+1})R(a)+R(\epsilon^{j+1})I(a) = \frac{\epsilon^{j+1}-\bar{\epsilon}^{j+1}}{2\sqrt{2}}\,a+\frac{\epsilon^{j+1}+\bar{\epsilon}^{j+1}}{2}\,b,$$

$$n_j = I(a\epsilon^j) = I(\epsilon^j)R(a)+R(\epsilon^j)I(a) = \frac{\epsilon^j-\bar{\epsilon}^j}{2\sqrt{2}}\,a+\frac{\epsilon^j+\bar{\epsilon}^j}{2}\,b\,.$$

The formulae in (4) follow from (2) in exactly the same manner.

In Theorem 5.4 it was shown that the sequences $\{T_j(p)\}$ and $\{T'_j(p)\}$ were disjoint. With Theorem 5.5 it is possible to show that these sequences are exhaustive in the sense that they contain every primitive pythagorean triple (x,y,z) with $|x-y| = p$. To prove this result, stated below as Theorem 5.6, it will be shown that if (x,y,z) has $|x-y| = p$, then its generators must be the same as those listed in Theorem 5.5.

Theorem 5.6. Let p be a rational prime of the form $8k \pm 1$. If $T = (x,y,z)$ is a primitive pythagorean triple such that $|x-y| = p$, then T is in one of the sequences $\{T_j(p)\}$ or $\{T'_j(p)\}$.

Proof. Let $u = a$, $v = b$ be the fundamental solution of $u^2-2v^2 = p$ and let $\alpha = a+b\sqrt{2}$. If m and n are the generators of $T = (x,y,z)$ then

$$y-x = (m-n)^2-2n^2.$$

Hence

$$N(\alpha) = p = \pm N([m-n] + n\sqrt{2}).$$

Since α is a prime, it follows that either α or $\bar{\alpha}$ is an associate of

$$(m-n) + n\sqrt{2}.$$

If α is an associate of $(m-n)+n\sqrt{2}$, then by definition there is an integer t such that

$$\alpha\epsilon^t = (m-n) + n\sqrt{2},$$

or

$$-\alpha\epsilon^t = (m-n) + n\sqrt{2}.$$

This second equality is impossible because

$$-\alpha\epsilon^t < 0 < (m-n) + n\sqrt{2}.$$

Thus if α is an associate of $(m-n)+n\sqrt{2}$, then

$$\alpha\epsilon^t = (m-n) + n\sqrt{2}$$

for some integer t. Note that $t < 0$ implies that

$$\alpha > \alpha\epsilon^t = (m-n) + n\sqrt{2} \geqslant a + b\sqrt{2} = \alpha,$$

which is a contradiction. Thus if α is an associate of $(m-n)+n\sqrt{2}$, there is an integer $t \geqslant 0$ such that

$$\alpha\epsilon^t = (m-n) + n\sqrt{2}.$$

It is now clear that, in this case, T is generated by

$$m = R(\alpha\epsilon^t) + I(\alpha\epsilon^t)$$

and

$$n = I(\alpha\epsilon^t),$$

with $t \geqslant 0$, so that T is in $\{T_j(p)\}$.

If $\bar{\alpha}$ is an associate of $(m-n)+n\sqrt{2}$, then by definition, there exists an integer t such that

$$\bar{\alpha}\epsilon^t = (m-n) + n\sqrt{2},$$

or

$$-\bar{\alpha}\epsilon^t = (m-n) + n\sqrt{2}.$$

This last equality is impossible, because $\alpha > 0$ and $\alpha\bar{\alpha} = p$ imply that $\bar{\alpha} > 0$, and hence

$$-\bar{\alpha}\epsilon^t < 0 < (m-n) + n\sqrt{2}.$$

Note that if

$$\bar{\alpha}\epsilon^t = (m-n) + n\sqrt{2} \quad \text{and} \quad t \leqslant 0,$$

then

$$\bar{\alpha} \geqslant \bar{\alpha}\epsilon^t = (m-n) + n\sqrt{2} \geqslant a + b\sqrt{2} = \alpha > \bar{\alpha},$$

which is impossible.

Thus if $\bar{a}$ is an associate of $(m-n)+n\sqrt{2}$, then there is an integer $t>0$ such that

$$\bar{a}\epsilon^t = (m-n)+n\sqrt{2}\ .$$

Clearly, in this case, T is generated by

$$m = R(\bar{a}\epsilon^t)+I(\bar{a}\epsilon^t) \qquad \text{and} \qquad n = I(\bar{a}\epsilon^t),$$

with $t>0$, so that T is in $\{T_j'(p)\}$. This completes the proof.

In the description of the two sequences $\{T_j(p)\}$ and $\{T_j'(p)\}$ it is obvious that the sequence $\{T_j'(p)\}$ is closely related to the unique primitive pythagorean triple (x,y,z) with $x+y=p$. The following theorem is used to show that the sequence $\{T_j(p)\}$ is also related to the unique primitive pythagorean triple (x,y,z) with $x+y=p$.

Theorem 5.7. If m and n $(m>n)$ generate a primitive pythagorean triple (x,y,z), then $M=2n+m$ and $N=n$ generate a primitive pythagorean triple (X,Y,Z) such that $|X-Y|=x+y$.

The proof is computational and is left to the reader.

If p is a prime of the form $8k\pm 1$, then as in Theorem 4.2, the unique primitive pythagorean triple (x,y,z) with $x+y=p$, is generated by $m=a-b$ and $n=b$, where $u=a$, $v=b$ is the fundamental solution of $u^2-2v^2=p$. By Theorem 5.7,

$$M = 2n+m = a+b \qquad \text{and} \qquad N = n = b$$

generate a primitive pythagorean triple (X,Y,Z) such that

$$|X-Y| = x+y = p.$$

An examination of the generators M and N shows that (X,Y,Z) is the triple labeled $T_0(p)$ in the discussion of $\{T_j(p)\}$.

6. SUMMARY

In this paper it has been shown that the sum and the difference of the legs of a primitive pythagorean triple must be of the form $8k\pm 1$. Conversely, if p is a prime of the form $8k\pm 1$, there is a unique primitive pythagorean triple (x,y,z) with $x+y=p$, but there are two infinite disjoint sequences of primitive pythagorean triples with the difference of the legs equal to p for each triple in the sequences. Furthermore, every primitive pythagorean triple (x,y,z) with $|x-y|=p$ is in one of these sequences. Figure 2 outlines a general method for constructing these triples and Fig. 3 illustrates the procedure with $p=137$. Finally, explicit formulae for the generators of each triple in the sequences are given in terms of the fundamental solution of $u^2-2v^2=p$.

REFERENCES

1. L.E. Dickson, *History of the Theory of Numbers,* Vols. I and II, Chelsea, New York, N.Y., 1966.
2. G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers,* 4th ed., Clarendon Press, Oxford, 1960.
3. T. Nagell, *Introduction to Number Theory,* Chelsea, New York, N.Y., 1964.
4. L.W. Reid, *The Elements of the Theory of Algebraic Numbers,* Macmillan, New York, N.Y., 1910.
5. W. Sierpinski, "Pythagorean Triangles," *Scripta Mathematica Studies,* No. 9, Yeshiva University, New York, N.Y., 1962.
6. W. Sierpinski, *Elementary Theory of Numbers,* Panstwowe Wydawnnictwo Naukowe, Poland, 1964.
7. W. Sierpinski, *A Selection of Problems in the Theory of Numbers,* Pergamon Press, Macmillan, New York, N.Y., 1964.
8. W.P. Whitlock, Jr., "Pythagorean Triangles with a Given Difference or Sum of Sides," *Scrip. Math.,* Vol. II (1945), pp. 75–81.

****