A SECOND VARIATION ON A PROBLEM OF DIOPHANTUS AND DAVENPORT*

BURTON W. JONES
University of Colorado, Boulder, Colorado 80309

1. INTRODUCTION

In a paper appearing in the *Quarterly Journal of Mathematics* [Vol. 20 (1969), pp. 129–137], Harold Davenport and Alan Baker dealt with the set of numbers: 1, 3, 8, 120. It has the property, noted by Fermat, that the product of any two increased by one is a square. We call such a set a P-set. Davenport and Baker proved, using the "effective" results of the latter, that if 1, 3, 8, c is a P-set, then c must be 120.

Long before, Diophantus noticed that the set x, $x+2$, $4x+4$, $9x+6$ is a P-set for $x = 1/16$. Indeed, the first three have the same property considered as polynomials in x. In a previous paper [*Quar. Jour. Math.*, Vol. 27 (1976), pp. 349–353] the author proved that the only P-sets containing x and $x+2$ in $Z[x]$ are

$$x, \quad x+2, \quad c_r(x), \quad c_{r+1}(x),$$

where r is a positive integer and the c_i are certain polynomials defined recursively.

Here we consider a similar problem in a more general setting. Let $a = a(x)$ and $b = b(x)$ be two non-zero polynomials in $Z[x]$ such that $ab + 1 = w^2$, where w is in $Z[x]$. [We omit the argument x when there is no ambiguity.] Without loss, we may assume that a, b, and w are in $Z^+[x]$, that is, have positive leading coefficients. We want to allow a and b to be in Z; in this case $Z^+[x]$ becomes the set of positive integers.

First we seek all solutions $c_k = c_k(x)$ in $Z^+[x]$ of

$$(1.1) \qquad ac_k + 1 = y_k^2, \quad bc_k + 1 = z_k^2, \quad y_k \text{ and } z_k \text{ in } Z^+[x]\,.$$

An equivalent pair of equations is

$$(1.2) \qquad (b-a)c_k = z_k^2 - y_k^2, \quad b - a = by_k^2 - az_k^2\,.$$

In the previous paper we considered the case when $b = a+2$. Then there was just one sequence of c_k. If $b \neq a+2$, there are at least two such sequences. We prove that if a, b, and c form a P-set and all are of the same positive degree, then there is no fourth of the same degree which, with a, b, and c, forms a P-set. We prove that if a and b are both linear or quadratic there are exactly two sequences. If a and b are in Z and $a < b < 4a$ we prove that there are exactly two sequences of c_k (unless $b = a+2$); we also show that if $a < b < c < d$ form a P-set, then $d > ab + 1$. Our most significant result is that when a and b are linear over $Z^+[x]$, $c = a + b + 2w$, and a, b, c, d form a P-set of four elements, then there is exactly one possible d, namely

$$c_2(a,b) = (4w^2 - 2)c + 2(a+b),$$

where $ab + 1 = w^2$. The proof of this result is an adaptation of one of B. J. Birch given in the previous paper. We show that if a and b are two successive even-indexed Fibonacci numbers, $c_2(a,b)$ reduces to $4b(b^2+1)$ and is not a Fibonacci number. A final section describes some results which seem true but for which we have no proofs.

Since much of the theory is the same for integers and polynomials it is convenient to define an extension of the idea of inequality from integers to polynomials in $Z[x]$.

Definition. When we write "a is in $Z[x]$" we mean that it is either a polynomial of positive degree or an integer. In the latter case, we call it its own "leading coefficient." The symbol $a > 0$ means that the leading coefficient of a is positive. Similarly if a and b are in $Z[x]$, $a > b$ means that $a - b > 0$. The usual fundamental properties of inequality hold for this extension.

We assume throughout that

---

*The author promises there will not be a third; he has no intention of composing a sonata.

(1.3) $$0 < a < b.$$

If $n_a = \deg a$ denotes the degree of a in x, and similarly for n_b, then (1.3) implies $n_a \leqslant n_b$. Note that n_a and n_b must be of the same parity and $2n = n_a + n_b$, where $n = n_w$. Define c_0 to be 0 and have as a consequence that $y_0 = z_0 = 1$.

2. FORMULAS FOR c_k IN (1.1) AND (1.2)

In order to find a formula for c_k we first seek a recursion formula for y_k and z_k. To this end, write

(2.1) $$(\sqrt{b}\,y_k + \sqrt{a}\,z_k = (w + \sqrt{ab})(\sqrt{b}\,y_{k-1} + \sqrt{a}\,z_{k-1}),$$

that is

(2.2) $$\begin{aligned} y_k &= wy_{k-1} + az_{k-1} \\ z_k &= by_{k-1} + wz_{k-1}. \end{aligned}$$

To see that (2.2) defines a sequence of solutions of (1.1) suppose that y_{k-1}, z_{k-1} is a solution of the second equation of (1.2). In (2.1) replace $\sqrt{a}$ by $-\sqrt{a}$ and multiply corresponding sides of the two equations to get:

$$by_k^2 - az_k^2 = (w^2 - ab)(by_{k-1}^2 - az_{k-1}^2).$$

Another way to show this is to use Eqs. (2.2) directly in the second equation of (1.2). We show below that the first equation of (1.2) defines c_k.

Now $wy_k - az_k = y_{k-1}$ which implies

$$y_k = wy_{k-1} + wy_{k-1} - y_{k-2} = 2wy_{k-1} - y_{k-2}.$$

Also $wz_k - by_k = z_{k-1}$ implies $z_k = 2wz_{k-1} - z_{k-2}$. So

(2.3) $$y_k - 2wy_{k-1} + y_{k-2} = 0 \quad \text{and} \quad z_k - 2wz_{k-1} + z_{k-2} = 0.$$

Note that $y_1 = w + a$ and $z_1 = b + w$ with (1.2) imply that $c_1 = 2w + a + b$. By induction, $\deg y_k = kn$. Hence, from (1.1) $\deg c_k = 2kn - n_a$, if $k > 0$, and $\deg z_k = (k+1)n - n_a$.

Let α and α^{-1} be the zeroes of $e^2 - 2we + 1$. Thus

$$\alpha = w + \sqrt{ab} \quad \text{and} \quad \alpha^{-1} = w - \sqrt{ab}.$$

Note that $ab \neq 0$ implies that $w \neq 1$. We seek y_k, z_k, and c_k in terms of α and α^{-1}. Thus we want to determine r and s so that

$$y_k = \frac{r\alpha^k - s\alpha^{-k}}{\alpha - \alpha^{-1}}.$$

Now $r - s = \alpha - \alpha^{-1}$ and $r\alpha - s\alpha^{-1} = (w+a)(\alpha - \alpha^{-1})$. This shows that

$$r = w + a - \alpha^{-1} \quad \text{and} \quad s = w + a - \alpha.$$

Hence

$$y_k = (w+a)f_k - f_{k-1} \quad \text{and, similarly,} \quad z_k = (w+b)f_k - f_{k-1},$$

where

$$f_k = \frac{\alpha^k - \alpha^{-k}}{\alpha - \alpha^{-1}}.$$

Thus we have

$$(z_k - y_k)(z_k + y_k) = (b-a)f_k[(2w + a + b)f_k - 2f_{k-1}].$$

Recalling that $c_1 = a + b + 2w$, we have, from (1.2),

(2.4) $$c_k = f_k(c_1 f_k - 2f_{k-1}).$$

It is interesting and useful to find a recursion formula for c_k. To this end note that $e^2 - 2we + 1 = 0$ implies

$$e^4 - (4w^2 - 2)e^2 + 1 = 0.$$

Thus

(2.5) $$(\alpha^{\pm 2})^k - (4w^2 - 2)(\alpha^{\pm 2})^{k-1} + (\alpha^{\pm 2})^{k-2} = 0, \quad \text{for } k \geqslant 2.$$

Then $f_k^2 = \alpha^{2k} + \alpha^{-2k} + N$, where N is independent of k, and (2.5) implies

$$f_k^2 = (4w^2-2)f_{k-1}^2 - f_{k-2}^2 + N', \tag{2.6}$$

where N' is independent of k. Furthermore

$$(f_k + f_{k-1}) - 2w(f_{k-1} + f_{k-2}) + (f_{k-2} + f_{k-3}) = 0$$

implies that $(f_k + f_{k-1})^2$ satisfies the same recursion formula as f_k^2 except for a change in N'. Thus $2f_kf_{k-1}$ and f_kf_{k-1} satisfy the same recursion formula except for the term independent of k. Thus

$$c_k = (4w^2-2)c_{k-1} - c_{k-2} + L,$$

where L is in $Z[x]$ and is independent of k. Taking $k = 2$, we have

$$c_2 = (4w^2-2)c_1 + L.$$

On the other hand, (2.4), $f_2 = 2w$, and $f_1 = 1$ imply

$$c_2 = 4w^2c_1 - 4w. \tag{2.7}$$

This shows that $L = 2c_1 - 4w = 2(a+b)$. Hence we have

$$c_k = (4w^2-2)c_{k-1} - c_{k-2} + 2(a+b). \tag{2.8}$$

This is the recursion formula we sought.

3. UNIQUENESS OF SOLUTIONS

We could hope that the c_k as developed above would be the only solutions of the Eqs. (1.1) and (1.2), but this is not so in general. However the c_k are the only solutions if $b - a = 2$ and, with one exception, when a and b are both linear polynomials. To show this we develop a useful algorithm.

Let a, b, c be three polynomials in $Z^+[x]$ such that $a < b$ and

$$ab + 1 = w^2, \quad ac + 1 = y^2, \quad bc + 1 = z^2, \quad \text{with} \quad x,y,z \text{ in } Z^+[x]. \tag{3.1}$$

Replacing $y_k, z_k, y_{k-1}, z_{k-1}$ in (2.2) by y, z, y', z', respectively, we have the transformation:

$$y = wy' + az', \qquad z = by' + wz' \tag{3.2}$$

and its inverse,

$$y' = wy - az, \qquad z' = -by + wz. \tag{3.3}$$

This transformation is an automorph of $by^2 - az^2$, that is, $by'^2 - az'^2 = by^2 - az^2$. We now show that if $b \leqslant a + c$ and if c satisfies (3.1), then (3.3) yields a $c' < c$. This is the basis of our algorithm.

First we show that y' is in $Z^+[x]$ without further condition on a, b, and c except those in (3.1). Also z' is in $Z^+[x]$ if and only if $b \leqslant a + c$. From the second equation of (1.2) with subscripts suppressed, we have

$$a(b-a) = (w^2-1)y^2 - a^2z^2,$$

that is,

$$a(b-a) + y^2 = (wy - az)(wy + az).$$

Since $b > a$, the left side is positive and since y and z are positive, $wy + az$ is positive. Hence

$$wy - az = y' > 0.$$

Similarly,

$$b(b-a) = b^2y^2 - (w^2-1)z^2,$$

which shows that

$$(wz - by)(wz + by) = z^2 - b(b-a) = 1 + b(c + a - b) > 0$$

if and only if $b \leqslant a + c$. Thus

$$wz - by = z' > 0 \quad \text{if and only if} \quad b \leqslant a + c.$$

Second, we show that y' and z' define a c' in $Z[x]$ such that

(3.4) $$ac' + 1 = y'^2 \quad\text{and}\quad bc' + 1 = z'^2.$$

To this end we compute

$$z'^2 - y'^2 = [(w-b)y + (w-a)z][(-w-b)y + (w+a)z] = (b-a)(by^2 + az^2) + z^2 - y^2 - 2w(b-a)yz$$
$$= (b-a)c', \quad\text{where}\quad c' = by^2 + az^2 + c - 2wyz.$$

Since $b - a = by'^2 - az'^2$, we have from the equivalence of equations (1.1) and (1.2) that Eqs. (3.4) hold.

Third, assume that b is of positive degree and $b \leqslant a + c$. Then w is of positive degree. As in the first part of our argument with y and y', z and z' interchanged, we have $wy' - az' > 0$. Hence (3.2) shows

(3.5) $$n_{y'} = n_y - n.$$

If $c' = 0$, then $b \leqslant a + c$ implies $y' = z' = 1$ and hence $n_y = n$ and $n_z = n_b$ from (3.2). If $c' \neq 0$, then, from (3.4)

$$n_a + n_{c'} = 2n_{y'} = 2n_y - 2n = n_a + n_c - 2n = 2n_z - 2n.$$

Hence the following holds

(3.6) If $c' \neq 0$, then $n_{c'} = n_c - 2n$ and $n_{z'} = n_z - n$.

Finally, suppose b is in Z and $b \leqslant a + c$. This implies that a and w are in Z. It also implies that c is in Z for if c were of positive degree with leading coefficient d, then (3.1) would imply that ad and bd would be squares; this is impossible if $ab + 1$ is a square. So if b is in Z, all the letters in (3.1) represent positive integers. As in the previous paragraph, $wy' - az' > 0$ which implies

(3.7) $$y' < y/w.$$

From (3.4) we have, using (3.7),

$$ac' = y'^2 - 1 < y^2/w^2 - 1 = (ac+1)/w^2 - 1 < ac/w^2,$$

since $w > 1$. Hence

(3.8) $$0 \leqslant c' < c/w^2.$$

We collect all these results in the following theorem.

Theorem 1. Let a, b, c be a P-set over $Z^+[x]$ with $a < b$, let y and z in $Z^+[x]$ be defined by (1.1) with subscripts suppressed, and y' and z' defined by (3.3). Then $c' = by^2 + az^2 - 2wyz + c$ defines a c' such that a, b, c' is a P-set and (3.4) holds. Also $y' > 0$ without further condition, and $z' > 0$ if and only if $b \leqslant a + c$. If b is of positive degree and $b \leqslant a + c$, then conditions (3.5) and (3.6) hold. If b is in Z and $b \leqslant a + c$, then (3.7) and (3.8) hold. [Inequality (3.8) is sharpened in Lemma 4 of Section 6.]

The results of Theorem 1 provide the mechanism to prove two useful theorems.

Theorem 2. If $a < b < c$ are polynomials of the same degree over $Z^+[x]$ which satisfy Eqs. (3.1) and, when a, b, c are in Z, the additional condition $c \leqslant w^2 = ab + 1$ holds, then $c = a + b + 2w = c_1(a,b)$.

Proof. The conditions of the theorem imply that $n_a = n = n_c$ and $b < a + c$. If $n > 0$, $n_c = n$ and (3.6) imply $c' = 0$. If $n = 0$, (3.8) implies $c' = 0$. In both cases $y' = z' = 1$ and (3.2) shows that $y = w + a$, $ac + 1 = y^2$ and hence $c = a + b + 2w$. This completes the proof.

Corollary 1. If a,b,c,d are four distinct polynomials of equal positive degree over $Z^*[x]$ they do not form a P-set.

The corollary follows since if they form a P-set we may take $a < b < c < d$ and see from Theorem 2 that $c = d$, which is a contradiction.

The corresponding result for a and b in Z is the following.

Corollary 2. If a and b are in Z with $a < b$ and if $a < b < c < d$ form a P-set, then $d > ab + 1$. [In view of Lemma 4 in Section 6, $d > ab + 1$ could be replaced by $d > 4ab$.]

A closely allied result is the following.

Theorem 3. If $4a > b > a$, $ab + 1 = w^2$, and $a < c < b$, then a, b, c do not form a P-set in $Z^+[x]$.

Proof. Note that the conditions $4a > b > a$ and $a < c < b$ imply that a, b, c are polynomials of the same degree. If $c > 4$, $b < 4a$ implies $b < ac + 1$ and hence from Theorem 2 with b and c interchanged,

$$b = a + c + 2w', \quad \text{where} \quad w'^2 = 1 + ac.$$

Then

$$ab + 1 = a^2 + ac + 2aw' + 1 = (a + w')^2 = w^2$$

implies $w' = w - a$ and $c = a + b - 2w$. But $c > a$ implies $b(b - 4a) > 4$ which denies $b < 4a$. If $c \leqslant 3$ it is easy to complete the proof.

Theorem 3 affirms that if a and b are "close enough together," whether of positive degree or in Z, then no c can be inserted between a and b to form a P-set of three elements.

Now we assume that a and b are of the same *positive* degree and seek all c satisfying (3.1). [In Section 6 we consider the same problem for a and b in Z.] We can get explicit results if $n_c = kn$, where $n = n_a = n_c$. Since each time we apply transformation (3.3), Theorem 1 shows that we decrease the degree of c by $2n$, we eventually arrive at a $\tilde{c}$ of degree n or in Z according as k is odd or even. Then if $b < \tilde{c}$, Theorem 2 shows that $\tilde{c} = c_1(a,b) = a + b + 2w$ and hence $c = c_k(a,b)$ for some k. If, on the other hand, $\tilde{c} < b$ we consider two cases separately.

First if $\tilde{c} < b$ and $\tilde{c}$ is of positive degree n, Theorem 2 with b and $\tilde{c}$ interchanged shows that $b = a + \tilde{c} + 2\tilde{y}$ where $\tilde{y}^2 = a\tilde{c} + 1$. As in the proof of Theorem 3, this implies $\tilde{c} = a + b - 2w$. This leads to a whole new sequence which we designate by $\bar{c}_j$. We can compute the members of this sequence by going back to Section 2 and starting with $y_0 = 1 = -z_0$ in place of $y_0 = 1 = z_0$. Then y_k and z_k will satisfy the same recursion formula but will be expressed differently in terms of the f_k. Using an argument similar to that of Section 2 it can be found that

$$\bar{c}_k(a,b) = f_k(\bar{c}_1 f_k + 2f_{k-1}), \quad \text{where} \quad \bar{c}_1 = a + b - 2w. \tag{3.9}$$

It can also be verified that the $\bar{c}_j$ satisfy the same recursion formula as c_k, given in (2.8).

Second, if $\tilde{c} < b$ and $\tilde{c}$ is in Z, then $\tilde{c} < a < b$ and n is even. If $\tilde{c} = 0$, then $\tilde{y} = 1 = \tilde{z}$, the c before $\tilde{c}$ is $c_1(a,b)$ and $c = c_k(a,b)$ for some k. Then it remains to consider $0 < \tilde{c} < a < b$. Now, since $a < b + \tilde{c}$ we may use Theorem 1 with $\tilde{c}, a, b$ in place of a, b, c. Since $\tilde{c}a + 1 = \tilde{y}^2$, $\tilde{c}b + 1 = \tilde{z}^2$, and $ab + 1 = w^2$ we define z' and w' by what corresponds to (3.3), namely

$$z' = \tilde{y}\tilde{z} - \tilde{c}w$$
$$w' = a\tilde{z} - \tilde{y}w.$$

By Theorem 1, $\tilde{c}b' + 1 = z'^2$ defines b' which, by (3.6), must be in Z. Now since $\tilde{c}b' + 1$, $\tilde{c}a + 1$, $b'a + 1$ are all squares with only a not in Z, the last paragraph in the proof of Theorem 1 implies that $b' = 0$. Hence $a < b + \tilde{c}$ implies $z' = w' = 1$ and $b = a + 2\tilde{y} + \tilde{c}$. But $w = a + \tilde{y}$. Hence $\tilde{c} = a + b - 2w$ and $c = \bar{c}_j(a,b)$ for some j. We collect these results in the next theorem.

Theorem 4. If a and b are of the same positive degree, c satisfies (3.1), and the degree of c is a multiple of n, then $c = c_k(a,b)$ for some k or $c = \bar{c}_j(a,b)$ for some j. The second sequence is omitted if $b = a + 2$.

Corollary. If a and b are both linear or both quadratic in x and if c satisfies (3.1), then $c = c_k(a,b)$ for some k or $c = \bar{c}_j(a,b)$ for some j. The second sequence is omitted if $b = a + 2$.

The corollary follows since if $n = 2$, the degree of c satisfying (3.1) must be even. When $n > 2$, we have in general more than two sequences. But by (3.3) we can for each c find a $\tilde{c}$ of degree not greater than n. From these $\tilde{c}$, stem all the c satisfying (3.1).

4. WHEN IS $c_k c_r + 1$ A SQUARE?

To answer this question we first find a formula for $c_k c_r + 1$ for $k > r$. Since we need a similar result for $\bar{c}_i$ we adopt a temporary notation which enables us to derive both results simultaneously. First, by use of $f_{k+1} = 2wf_k - f_{k-1}$, we can write (2.4) as

$$c_k = f_k(\bar{c}_1 f_k + 2f_{k+1}), \quad \text{where} \quad \bar{c}_1 = a + b - 2w. \tag{4.1}$$

Similarly, (3.9) can be written

$$\bar{c}_k = f_k(c_1 f_k - 2f_{k+1}). \tag{4.2}$$

To treat these together, we write

$$d_k = f_k(\bar{d}_1 f_k \pm 2f_{k+1}), \tag{4.3}$$

where $d_k = c_k$ or $\bar{c}_k$ according as $\pm$ is + or − and $\bar{\bar{d}}_1 = d_1$.

Then

$$d_k d_r + 1 = (\bar{d}_1 f_k f_r \pm f_{k+1} f_r \pm f_{r+1} f_k)^2 - (f_{r+1} f_k - f_{k+1} f_r)^2 + 1. \tag{4.4}$$

Now

$$\begin{vmatrix} f_{r+1} & f_r \\ f_{k+1} & f_k \end{vmatrix} = \begin{vmatrix} 2wf_r - f_{r-1} & f_r \\ 2wf_k - f_{k-1} & f_k \end{vmatrix} = \begin{vmatrix} f_r & f_{r-1} \\ f_k & f_{k-1} \end{vmatrix} = \begin{vmatrix} f_1 & f_0 \\ f_{k-r+1} & f_{k-r} \end{vmatrix} = f_{k-r}.$$

This shows that

$$f_{r+1} f_k - f_{k+1} f_r = f_{k-r}.$$

Thus

$$d_k d_r + 1 = (\bar{d}_1 f_k f_r \pm 2f_r f_{k+1} \pm f_{k-r})^2 - f_{k-r}^2 + 1. \tag{4.5}$$

Now if $k = r + 1$, it follows that $f_{k-r} = 1$ and we have

$$d_{r+1} d_r + 1 = (\bar{d}_1 f_{r+1} f_r \pm 2f_r f_{r+2} \pm 1)^2. \tag{4.6}$$

So we have the following theorem.

Theorem 5. The polynomials $c_{r+1} c_r + 1$ and $\bar{c}_{r+1} \bar{c}_r + 1$ are squares in $Z[x]$.

5. P-SETS WHEN a AND b ARE LINEAR

From Theorem 5, $c_k c_r + 1$ is a square when k and r are successive integers. If a and b are linear we can show as in the previous paper that $c_k c_r + 1$ is a square in $Z[x]$ only if k and r are consecutive integers. The idea of the argument is the same but the needed modifications cause a little trouble. We need the same result for $\bar{c}_k \bar{c}_r + 1$ but since the proof is almost the same, we omit it. We will need the following three lemmas which, as in the previous paper, we state without proof since the proofs are easy.

Lemma 1. Let $\varphi_1(a)$, $\varphi_2(a)$, and $\lambda(a)$ be three polynomials in $Z[a, a^{-1}]$ such that the first t coefficients of $\varphi_1(a)$ and $\varphi_2(a)$ are the same. Then the first t coefficients of $\varphi_1(a)\lambda(a)$ and $\varphi_2(a)\lambda(a)$ are the same.

Lemma 2. Let the first t coefficients of $\varphi_i(a)$ and $\psi_i(a)$ be the same for i = 1 and 2. Then the first t coefficients of $\varphi_1(a)\varphi_2(a)$ and $\psi_1(a)\psi_2(a)$ are also the same.

Lemma 3. Let $\varphi_i(a)$, i = 1, 2, be two polynomials in $Z[a, a^{-1}]$ whose leading coefficients are positive and such that the first t coefficients of their squares are the same. Then the first t coefficients of the two polynomials are the same.

Now we prove the basic theorem.

Theorem 6. If a and b are linear in $Z^+[x]$, with $ab + 1 = w^2$ and w in $Z^+[x]$, then a, b, c_r, c_k is a P-set if and only if r and k are consecutive integers. The same is true for $a, b, \bar{c}_r, \bar{c}_k$.

Proof. The "if" part is established by Theorem 5 and/or Eq. (4.6). To prove the "only if" part, first note that $e = a + b - 2w \geq 0$ is equivalent to $(b - a)^2 \geq 4$ with equality if and only if $b = a + 2$. So the case $e = 0$ is covered by the previous paper. Or the reader may prefer to note the modifications needed in the following proof where we assume that $e \neq 0$.

Now f_r can be thought of as a polynomial in $Z[a, a^{-1}]$ of degree $r - 1$. It has $2r - 1$ terms with 1 and 0 alternating as coefficients. Thus if $k > r$, the sequence of $2r - 1$ coefficients of f_r is the same as the sequence of the first $2r - 1$ coefficients for f_k. Henceforth in this proof we assume that $k > r + 1$, that $c_k c_r + 1$ is a square in $Z[x]$ and seek a contradiction. From what we have just noted, the first $2r + 1$ coefficients of $ef_k + 2f_{k+1}$ and of $ef_{r+1} + 2f_{r+2}$ are the same, where the f_i are viewed as polynomials in $Z[a, a^{-1}]$. Note that $e = a + b - 2w$, being different from zero, is not in Z, for suppose this is true and write

$$a = a_1 x + a_0, \quad b = b_1 x + b_0, \quad \text{and} \quad w = w_1 x + w_0.$$

Then if e is in Z, $a_1b_1 = w_1$ and $a_1 + b_1 - 2w_1 = 0$ imply $a_1 = b_1 = w_1$. From this it follows that $b_0 = a_0 + 2$ and hence $e = 0$, contrary to hypothesis. Furthermore e is not in $Z[\alpha, \alpha^{-1}]$ since α depends only on the product ab and not on the sum $a + b$. Let $Z' = Z[e]$ and see that c_k and c_r are in $Z'[\alpha^{-1}, \alpha]$.

Using Lemma 2 and (4.1) with $\bar{c}_1$ replaced by e, we then see that the first $2r + 1$ coefficients of c_k and c_{r+1} are the same. Then by Lemma 1, c_kc_r and $c_{r+1}c_r$ have the same first $2r + 1$ coefficients. Hence the same can be said for

$$g_{k,r} = c_kc_r + 1 \quad \text{and} \quad g_{r+1,r} = c_{r+1}c_r + 1.$$

Suppose $g_{k,r} = \varphi^2(x)$, that is, $g_{k,r}$ is a square in $Z[x]$. We next show that $g_{k,r}$ is also a square in $Z'[\alpha, \alpha^{-1}]$, in fact $\varphi(x) = \bar{e}\varphi_1 + \varphi_2$, where φ_1 and φ_2 are in $Z[\alpha, \alpha^{-1}]$ and $\bar{e}t' = e$ for some t' in Z. Note that $w_1 \neq 0$ since a and b are linear. Since $x = (w - w_0)/w_1$,

$$\varphi(x) = w_1^{-t}\sigma(w) = w_1^{-t}[w\sigma_0(w) + u],$$

where u is in Z, $t \geq 0$, and $\sigma(w)$ with $\sigma_0(w)$ are in $Z[w]$. Write $e = e_1x + e_0$ where, as we showed above, $e_1 \neq 0$. Note that $2w = \alpha + \alpha^{-1}$, and have

$$\begin{aligned}\varphi(x) &= e\sigma_1(\alpha)/e_1w_1^{t-1}2^s + \sigma_2(\alpha)/e_1w_1^t2^s\\ &= \bar{e}\sigma_3(\alpha)/v_1 + \sigma_4(\alpha)/v_2,\end{aligned}$$

where s is a non-negative integer, v_1 and v_2 are positive factors of $e_1w_1^t2^s$, no factor of v_1 greater than 1 divides all coefficients of $\bar{e}\sigma_3(\alpha)$ and no factor of v_2 greater than 1 divides all coefficients of $\sigma_4(\alpha)$. Let $v_1 = hv_3$, $v_2 = hv_4$, and $(v_3, v_4) = 1$. Then

$$h^2v_3^2v_4^2g_{k,r} = \bar{e}^2v_4^2\sigma_3^2 + 2\bar{e}v_3v_4\sigma_3\sigma_4 + v_3^2\sigma_4^2, \tag{5.1}$$

This implies that $v_4 | v_3^2$ and $v_3 | v_4^2$ and hence $v_4 = v_3 = 1$. Thus

$$h^2g_{k,r} = \bar{e}^2\sigma_3^2 + 2\bar{e}\sigma_3\sigma_4 + \sigma_4^2.$$

Hence $h^2 = 1$ and $\varphi(x) = \bar{e}\sigma_3(\alpha) + \sigma_4(\alpha)$, which is the result we announced at the beginning of this paragraph.

Now compare

$$\sqrt{g_{r+1,r}} = ef_{r+1}f_r + 2f_{r+2}f_r + 1,$$

from (4.6), and

$$\sqrt{g_{k,r}} = \bar{e}\sigma_3 + \sigma_4.$$

The degree of $\sqrt{g_{r+1,r}}$ in α is $2r$ and hence each of the first $2r$ coefficients of $\sqrt{g_{r+1,r}}$ is divisible by 2 or $\bar{e}$ (or both), and the first $2r + 1$-st coefficient is the term free of α. Now $f_{r+1}f_r$ is a sum of odd powers of α and hence there is no term free of α in $f_{r+1}f_r$. This, with (4.6) shows that the $2r + 1$-st coefficient of $g_{r+1,r}$ is an odd integer. We showed above that the first $2r + 1$ coefficients of $g_{k,r}$ and $g_{r+1,r}$ are the same. Hence, by Lemma 3, the $2r + 1$-st coefficient in $\sqrt{g_{k,r}}$ is an odd integer.

On the other hand, (4.3) with $d_i = c_i$, $\bar{d}_1 = \bar{c}_1 = e$ implies

$$\varphi^2(x) = g_{k,r} = e^2f_k^2f_r^2 + 2ef_kf_r(f_rf_{k+1} + f_kf_{r+1}) + 4f_kf_rf_{k+1}f_{r+1} + 1.$$

The degree of $g_{k,r}$ in α is $2r + 2k - 2$. Thus each of the first $2r + 2k - 2$ coefficients is divisible by $\bar{e}$ or 2. But

$$r + k - 1 \geq r + r + 2 - 1 = 2r + 1.$$

This is the contradiction that proves the theorem for c_k and c_r. The proof for $\bar{c}_k$ and $\bar{c}_r$ is almost the same.

Now we prove our principal theorem for a and b linear.

Theorem 7. Let a and b be linear in $Z^+[x]$ and $ab + 1 = w^2$, w in $Z^+[x]$. If

$$a, b, a + b + 2w, c \tag{5.2}$$

is a P-set of four elements, then

$$c = c_2(a,b) = \bar{c}_2(b, a + b + 2w). \tag{5.3}$$

Proof. Since a, b, c is a P-set, the corollary of Theorem 4 shows that $c = c_k(a,b)$ for some k or $c = \bar{c}_j(a,b)$ for some j. Now $a + b + 2w = c_1(a,b)$ and if $c = c_k(a,b)$, Theorem 6 implies

(5.4) $$c = c_2(a,b) \quad\text{or}\quad c = \bar{c}_j(a,b) \quad \text{for some } j.$$

Now use the same argument with a replaced by b and b by $a + b + 2w$. The corollary of Theorem 4 shows that $c = c_k(b, a + b + 2w)$ for some k or $c = \bar{c}_j(b, a + b + 2w)$ for some j. But

(5.5) $$a = \bar{c}_1(b, a+b+2w)$$

and Theorem 6 shows that

(5.6) $$c = \bar{c}_2(b, a+b+2w) \quad\text{or}\quad c = c_k(b, a+b+2w)$$

for some k.

Next we prove that $\bar{c}_2(b, a+b+2w) = c_2(a,b)$. Now $b(a+b+2w) + 1 = (b+w)^2$. So, using the recursion formula (2.8) for $\bar{c}$ in place of c, we have

$$\begin{aligned}\bar{c}_2(b, a+b+2w) &= [4(b+w)^2 - 2]a + 2(a+2b+2w)\\ &= [4(ab+b^2+2bw+1) - 2]a + 2(a+b+2w) + 2b\\ &= (4ab+2)(a+b+2w) + 2a + 2b\\ &= (4w^2-2)c_1(a,b) + 2a + 2b = c_2(a,b).\end{aligned}$$

Then if $c \neq c_2(a,b)$ we know from (5.3), (5.4), and (5.6) that $\bar{c}_j(a,b) = c_k(b, a+b+2w)$ for some j and k greater than 2. But since c_k is of degree $2k-1$ and c_j of degree $2j-1$, the equality implies $j = k$. We now reach a contradiction by showing that

(5.7) $$c_k(b, a+b+2w) > \bar{c}_k(a,b), \quad \text{if} \quad k > 2.$$

We showed above that $b(a+b+2w) + 1 = (b+w)^2$, that is, $b+w$ is the "w" for the pair $b, a+b+2w$. Corresponding to α for this pair is

$$\beta = b + w + \sqrt{(b+w)^2 - 1} > \alpha = w + \sqrt{w^2 - 1}.$$

Let $h_k = (\beta^k - \beta^{-k})/(\beta - \beta^{-1})$ to see that h_k corresponds to f_k. Thus, from (4.1) and (5.5)

$$c_k(b, a+b+2w) = h_k(ah_k + 2h_{k+1}).$$

Using (3.9), the inequality (5.7) may be written

(5.8) $$ah_k^2 + 2h_kh_{k+1} > (a+b-2w)f_k^2 + 2f_kf_{k-1}.$$

To show that (5.8) holds, it is sufficient to show that $ah_k^2 > (a+b-2w)f_k^2$ for $k \geq 2$. To this end we first show that h_k/f_k increases with k. To do this use the recursion formulas for h_k and f_k to get

$$\begin{aligned}h_kf_{k-1} - f_kh_{k-1} &> (2wh_{k-1} - h_{k-2})f_{k-1}(2wf_{k-1} - f_{k-2})h_{k-1}\\ &= h_{k-1}f_{k-2} - f_{k-1}h_{k-2} > h_2f_1 - h_1f_2 = h_2 - f_2 > 0.\end{aligned}$$

Hence h_k/f_k increases with k and (5.8) holds if

$$ah_2^2 > (a+b-2w)f_2^2, \quad\text{that is,}\quad a(b+w)^2 > (a+b-2w)w^2.$$

The last inequality is easy to verify. Hence the inequality (5.7) follows and the theorem is proved. The following corollary follows immediately from Theorem 2.

Corollary. Let a, b, d be a P-set of three linear elements of $Z^+[x]$ with $a < b < d$. Then the only P-set containing a, b, and d is

$$a, b, d, c_2(a,b).$$

REMARK. Notice that the part of the above where we showed $c_2(a,b) = \bar{c}_2(b, a+b+2w)$ did not depend on a and b being linear. In the course of proving *this* result we only assumed $ab + 1 = w^2$ and (2.8) for c_k and $\bar{c}_j$.

6. P-SETS OVER Z

In this section we assume that a and b are positive integers, $a < b$, and $ab + 1 = w^2$, where w is a positive integer. Also, as in Theorem 3, we assume that a and b are "not too far apart," specifically, that $b < 4a$. We find all integers

c such that a, b, c is a P-set. Toward this end we first need to sharpen inequality (3.8) of Theorem 1.

Lemma 4. Let a, b, c satisfy Eqs. (3.1) and let (3.3) define y', and $ac' + 1 = y'^2$ define c'. Then, if $b \leqslant a + c$, it follows that

(6.1) $$c' < c/4ab.$$

Proof. As in the proof of Theorem 1, the condition $b \leqslant a + c$ implies that y' and z' are positive. Since $bc' + 1 = z'^2$ we have

$$ac + 1 = y^2 = (wy' + az')^2 = w^2ac' + ab + 1 + a^2(1 + bc') + 2way'z'.$$

Hence

$$c = (w^2 + ab)c' + b + a + 2wy'z' > 2abc' + a + b + 2\sqrt{ab}\sqrt{ab}\,c',$$

since $w = \sqrt{ab+1}$. Thus $c > 4abc'$ and the proof is complete.

The first part of the proof of the next theorem is like that of Theorem 4. After this, further details must be dealt with.

Theorem 8. If $a < b < 4a$, a and b are in Z^+. and Eqs. (3.1) hold, then $c = c_k(a,b)$ for some k or $c = \bar{c}_j(a,b)$ for some j. The set $\bar{c}_j$ is omitted if $b = a + 2$.

Proof. If $c \geqslant w^2$, then $c > b - a$ and, by Theorem 1, a sequence of transformations (3.3) yields a $c' < w^2$. [We assume that the c before c' in the sequence is not less than w^2. If $c < w^2$ the argument is what follows.] If $c' > b$, Theorem 2 shows that $c' = a + b + 2w = c_1(a,b)$ and hence $c = c_k(a,b)$ for some k. If, on the other hand, $c' < b$, Theorem 3 shows that $c' < a < b$. Then if $b \leqslant ac' + 1$, Theorem 2 implies $b = a + c' + 2w'$, where $w'^2 = ac' + 1$. Then, as in the proof of Theorem 3, $c' = a + b - 2w$ and hence $c = \bar{c}_j(a,b)$ for some j, where this sequence is omitted if $c' = 0$, that is, if $b = a + 2$.

It remains to consider $0 < c' < a < b$ and $b > ac' + 1$. Then $4a > b$ implies $c' \leqslant 3$. Write $ac' + 1 = y'^2$ and $bc' + 1 = z'^2$. Now we use (3.3) once for c', a, b in place of a, b, c. By Lemma 4 the transformation takes b into b' satisfying the inequality

$$b' < b/4ac' < 1/c',$$

since $a < 1 + b$. Hence $b' = 0$ and, as in Theorem 2, this implies

(6.2) $$b = a + c' + 2y' = c_1(c', a).$$

First if $c' = 2$ or 3, $b > ac' + 1$ implies $a + c' + 2y' > ac' + 1$. Then

$$2y' > da - d, \quad \text{where} \quad d = c' - 1.$$

Then

$$4(ac' + 1) > d^2a^2 - 2d^2a + d^2,$$

(6.3) $$0 > d^2a^2 - 2a(d^2 + 2d + 2) + d^2 - 4.$$

If $d = 2$, (6.3) becomes $0 > 4a^2 - 20a$, that is, $a < 5/2$ which is impossible. If $d = 1$, (6.3) becomes $0 > a^2 - 10a - 3$ which holds if and only if $a \leqslant 10$. Then, under the conditions imposed, the only possibility is $a = 4$, $b = 12$, $w = 7$. Then $a + b - 2w = 2 = c' = \bar{c}_1(a,b)$ and $c = \bar{c}_j(a,b)$ for some j.

Second, if $c' = 1$, (6.2) becomes $b = a + 1 + 2y'$ and $1 + ab = w^2$ implies $w = y' + a$. Hence $a + b - 2w = c' = \bar{c}_1(a,b)$. Then, as in the case when $d = 1$, $c = \bar{c}_j(a,b)$ for some j. This completes the proof.

Theorem 8 implies the following theorem with only two little details to be filled in.

Theorem 9. If $a, b, e = a + b + 2w, d$ is a P-set of four distinct elements of Z^+ subject to the conditions $a < b < 4a$ and $ab + 1 = w^2$, then d must be in each of the two following sets:

$$\mathcal{S}_1 = \{c_k(a,b) \quad \cup \quad \bar{c}_j(a,b)\}$$
$$\mathcal{S}_2 = \{c_k(b,e) \quad \cup \quad \bar{c}_j(b,e)\}.$$

One possibility is $d = c_2(a,b) = \bar{c}_2(b,e)$. If $b = a + 2$, then $\mathcal{S}_1 = \{c_k(a,b)\}$.

Proof. To apply Theorem 8 to this theorem we must notice that $e < 4b$ is equivalent to $4 < (9b - a)(b - a)$ which holds since $b > a > 0$. For the rest, one notes the Remark after the Corollary of Theroem 7.

7. P-SETS OF FIBONACCI NUMBERS

Let F_i denote the i^{th} Fibonacci number. The following well known facts can easily be verified for $a = F_{2r-2}$, $b = F_{2r}$, $r > 1$:

i) $w^2 = ab + 1 = (b-a)^2$, that is, $a^2 - 3ab + b^2 = 1$.

ii) If $e = F_{2r+2}$, then $e = c_1(a,b) = 3b - a$, $ae + 1 = (a+w)^2 = b^2$, $be + 1 = (b+w)^2 = (2b-a)^2$, where

$$w = b - a = F_{2r-1}.$$

These two properties show that a, b, e form a P-set. From i),

$$b = at, \quad \text{where} \quad 2t = 3 + \sqrt{5 + 4/a^2}. \tag{7.1}$$

This shows that $b \leqslant 3a$ with equality only if $a = 1$. Hence the hypotheses of Theorem 8 hold and all the numbers d such that a, b, e, d form a P-set can be expressed as $c_k(a,b)$ or $\bar{c}_j(a,b)$. V. E. Hoggatt, Jr., and C. E. Bergum showed [1] that

$$F_{2r-2}, F_{2r}, F_{2r+2}, c = 4F_{2r-1}F_{2r}F_{2r+1} \tag{7.2}$$

is a P-set. It is not hard to show that c in (7.2) is, in our notation, $c_2(a,b)$ for $a = F_{2r-2}$ and $b = F_{2r}$. To this end, notice that, since $F_{2r-1}F_{2r+1} = F_{2r}^2 + 1$, c in (7.2) can also be written

$$c = 4b(b^2+1), \quad \text{where} \quad b = F_{2r}. \tag{7.3}$$

This can be shown to be $c_2(a,b)$ by using (2.8) with $w = b - a$, $k = 2$.

Our Theorem 3 shows that there is no c between F_{2r-2} and F_{2r} such that c, F_{2r-2}, F_{2r} is a P-set. Theorem 2 shows that if these same three numbers form a P-set with $F_{2r} < c < F_{2r-1}^2$, then $c = F_{2r+2}$. The following Theorem shows that c is not a Fibonacci number.

Theorem 10. If $a = F_{2r-2}$, $b = F_{2r}$, and $r > 1$, then

$$F_{6r-1} < c_2(a,b) < F_{6r}. \tag{7.4}$$

Proof. From (7.3), $c_2(a,b) = 4F_{2r}^3 + 4F_{2r}$. Now

$$F_k = \frac{\beta^k - \bar{\beta}^k}{\beta - \bar{\beta}}, \quad \text{where} \quad \beta = (1+\sqrt{5})/2,\ \bar{\beta} = (1-\sqrt{5})/2.$$

Hence

$$F_k^3 = \frac{F_{3k} - 3(-1)^k F_k}{(\beta - \bar{\beta})^2} = (1/5)[F_{3k} - 3(-1)^k F_k]. \tag{7.5}$$

Thus the two inequalities in (7.4) will follow if we can show

$$F_{6r}/F_{2r} > 8, \tag{7.6}$$

$$F_{6r}/F_{6r-1} > 5/4. \tag{7.7}$$

To show (7.6) use (7.5) to get $F_{6r}/F_{2r} = 5F_{2r}^2 + 3$, which shows that F_{6r}/F_{2r} is an increasing function of r. Then (7.6) follows from

$$F_{6r}/F_{2r} \geqslant F_{12}/F_4 = 48 > 8.$$

Also (7.7) holds since F_{2r}/F_{2r-1} is an increasing function of r and

$$F_{6r}/F_{6r-1} \geqslant F_{12}/F_{11} = 144/89 > 5/4.$$

Thus the proof is complete.

8. UNFINISHED BUSINESS

For b of degree greater than 2, there does not seem to be much of interest since in most cases there will be more than two sequences of numbers which with a and b form a P-set. For a and b linear it would be interesting to show that

$$a,\ b,\ c_r(a,b),\ \bar{c}_s(a,b) \tag{8.1}$$

is not a P-set for any r and s. The difficulty in proving this is that, if one is to use the method of Birch, one first needs a pair r,s for which $c_r\bar{c}_s + 1$ is a square. One might at least prove that there isat most one pair r and s such that (8.1) is a P-set.

For a and b quadratic functions of x, the basic difficulty is that $g_{k,r}$ could be a square in $Z[x]$ without being a square over $Z[a,b]$. Even if that were surmounted, adapting Theorem 6 to quadratics would present some difficulties.

For a and b integers, this paper does not add much to present knowledge except to place the problem in a larger setting. The Davenport-Baker result shows that in Theroem 9 when $a = 1$, $b = 3$, the intersection of $\mathcal{J}_1$ and $\mathcal{J}_2$ is $c_2(1,3) = 120$. A really significant result would be a proof that this is true for a and b any two successive Fibonacci numbers of even index. To show this independently from their result would present all the difficulties they encountered for their special case. At one time I hoped that one might by using the sequence of transformations (3.3) and a proof of "infinite descent" reduce the general result to that of the pair $a = 1$, $b = 3$, but it does not seem to work.

A somewhat weaker result would be the conjecture that if a, b, c are three successive even-indexed Fibonacci numbers and if a, b, c, d is a P-set of four numbers, then d cannot be a Fibonacci number. From Theorem 10, $c_2(a,b)$ is not a Fibonacci number. Unfortunately, for $c_k(a,b)$ with $k > 2$ there does not seem to be such a definite inequality as (7.4). One possible approach could be to consider the set of Fibonacci numbers as dividing the line of positive reals into intervals. Perhaps one could, using Theorem 9, assume, for example, that $c_r(a,b)$ and $c_s(b,e)$ were in the same interval and thus get a relationship between r and s which might be fruitful. But this seems like a long hard row to hoe. Also it would be interesting to show that a, b, c as defined above are not in a P-set of five elements. All of these results seem very plausible.

REFERENCE

1. V. E. Hoggatt, Jr., and G. E. Bergum, "A Problem of Fermat and the Fibonacci Sequence," *The Fibonacci Quarterly,* Vol. 15, No. 4 (Dec. 1977), pp. 323–330.

****

[Continued from page 154.]

B. We can easily obtain

$$\binom{2p}{p}p = 2(2p-1)\binom{2p-2}{p-1} \quad \text{and from Part A,} \quad \binom{2p}{p} \equiv 2 \pmod{p^3}.$$

Thus $2p \equiv 2(2p-1)\binom{2p-2}{p-1} \pmod{p^3}$. Since $(2,p^3) = (2p-1,p^3) = 1$, 2, and $2p-1$ we have the multiplicative inverses $\pmod{p^3}$ and we get $p/(2p-1) \equiv \binom{2p-2}{p-1} \pmod{p^3}$. Now $(2p-1)^{-1} \equiv -1-2p-4p^2 \pmod{p^3}$. Hence

$$p/(2p-1) \equiv p(-1-2p-4p^2) \pmod{p^3} \equiv -p-2p^2 \pmod{p^3}.$$

The result then follows.

AN ADJUSTED PASCAL

H-213 Proposed by V. E. Hoggatt, Jr., San Jose State University, San Jose, California.

A. Let A_n be the left adjusted Pascal triangle, with n rows and columns and 0's above the main daigonal. Thus

$$A_n = \begin{pmatrix} 1 & 0 & & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ 1 & 2 & 1 & 0 \cdot & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{pmatrix}_{n\times n}$$

Find $A_n \cdot A_n^T$ where A_n^T represents the transpose of matrix, A_n.

B. Let

$$C_n = \begin{pmatrix} 1 & 0 & 0 & & & \cdots & 0 \\ 0 & 1 & 0 & & & \cdots & 0 \\ 0 & 1 & 1 & 0 & & \cdots & 0 \\ 0 & 0 & 2 & 1 & 0 & \cdot & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \end{pmatrix}_{n\times n}$$