NNTDM 5 (1999) 4, 151-162

THE CARDANO FAMILY OF EQUATIONS

J.V. Leyendekkers

The University of Sydney, 2006, Australia

A.G. Shannon

University of Technology, Sydney, 2007, &
KvB Institute of Technology, North Sydney, NSW, 2060, Australia

ABSTRACT

The polynomial expansion of the Diophantine equation $x^n = (x-p)^n + (x-q)^n, p, q \in \mathbb{Z}_+, n > 2$, yields roots of the form $((p+q)+y)$ where y is a non-integer zero of a Cardano cubic polynomial of the form $y^3 - 6pqy - 3pq(p+q)$. This is a corollary to Fermat's Last Theorem. The characteristics of this family are illustrated for $n = 3, 4, \ldots, 9$. For n odd, y_0 can be represented by $(n-1)(2pq+e)^{\frac{1}{2}}$, and for n even there are two real values of y_0, $(n-1)(2pq+e)^{\frac{1}{2}}$ and $-(2pq+d)^{\frac{1}{2}}$, where d, e are real non-integer parameters. For a given n, e is simply related to $p/q, p < q$, and to a parameter E which is linear in n. The corresponding curves indicate the non-integral nature of $y, n > 2$.

1. INTRODUCTION

Babylonian mathematicians were familiar with cubic equations and the Iranian scholar Omar Khayyam (1048-1122) solved many cubic equations with the aid of algorithms with a conic section base [8]. However, in the West Geronimo Cardano (1501-1576) seems to have been the first to have published an analysis of the cubic equation [2]:

$$x^3 + Px + Q = 0 \tag{1.1}$$

though Cardano admitted that he had obtained the hint for this from Niccolo Tartaglia (c.1500-1557) [1]. The solution of Equation (1.1) is given by

$$x = [-\tfrac{1}{2}Q + (\tfrac{1}{4}Q^2 + \tfrac{1}{27}P^3)^{\frac{1}{2}}]^{\frac{1}{3}} + [-\tfrac{1}{2}Q - (\tfrac{1}{4}Q^2 + \tfrac{1}{27}P^3)^{\frac{1}{2}}]^{\frac{1}{3}}. \tag{1.2}$$

Equation (1.2) yields some interesting results. For example, with $P = -15$ and $Q = -4$,

$$x = [2 + (-121)^{\frac{1}{2}}]^{\frac{1}{3}} + [2 - (-121)^{\frac{1}{2}}]^{\frac{1}{3}}. \tag{1.3}$$

Cardano, unable to handle the square root of a negative number, called this result a *casus irreducibilis* because he knew that $x = 4$ is a solution. This result, with all roots real,

occurs when $27Q^2 + 4P^3$ is negative. When $27Q^2 + 4P^3 \geq 0$, one root is real and the other two form a complex conjugate pair.

In the present paper we show how a special form of the Cardano equation which does not yield integer solutions can be related to diophantine equations which lack integer solutions.

2. THE CUBIC CASE

Consider the diophantine equation

$$x^3 = (x-p)^3 + (x-q)^3,\ p, q \in \mathbb{Z}_+, \tag{2.1}$$

which can be rewritten as

$$x^3 - 3(p+q)x^2 + 3(p+q)x - (p^3 + q^3) = 0.$$

Now let

$$y = x - (p+q)$$

which is the standard way to produce

$$y^3 - 6pqy - 3pq(p+q) = 0.$$

the canonical form of the Cardano cubic [11].

Next consider the real-valued function z defined by

$$z = y^3 - 6pqy - 3pq(p+q). \tag{2.2}$$

Differentiation yields

$$\frac{dz}{dy} = 3y^2 - 6pq. \tag{2.3}$$

and so

$$y = \mp(2pq)^{\frac{1}{2}} \tag{2.4}$$

at the maximum and minimum where

$$z = \mp 4pq(2pq)^{\frac{1}{2}} - 3pq(p+q) \tag{2.5}$$

respectively. Since

$$3pq(p+q) > 6(pq)^{\frac{1}{2}} > 4pq(2pq)^{\frac{1}{2}}$$

z is always negative at these points as in Figure 1. (The figures are at the end of the paper.) We show next that z crosses the z-axis only once.

Put $P = -6pq, Q = -3pq(p+q)$, and the original equation has the form of a Cardano cubic equation:

$$0 = y^3 + Py + Q \tag{2.6}$$

Since

$$27Q^2 + 4P^3 = 27(pq)^2(9(p^2+q^2) - 14pq)),$$

and

$$9(p^2+q^2) > 7(p^2+q^2) > 14pq,$$

$$27Q^2 + 4P^3 \geq 0,$$

so that there are two complex conjugate roots, a_2, a_3, and one real root, a_1 [2]. The real solution, according to Cardano, is then

$$a_1 = \{\tfrac{1}{2}pq[3(p+q) + (9(p^2+q^2) - 14pq)^{\frac{1}{2}}]\}^{\frac{1}{3}} + \{\tfrac{1}{2}pq[3(p+q) - (9(p^2+q^2) - 14pq)^{\frac{1}{2}}]\}^{\frac{1}{3}}$$

Some examples are shown in Table 1.

p	q	a_1	x	E	e
2	1	4.0545588	7.0545588	0.0272794	0.1098618
2	3	6.9909756	11.9909756	0.0181208	0.2184349
2	5	9.1128667	16.1128667	0.0376989	0.7610848
3	4	9.8751505	16.8751505	0.0157567	0.3796493
3	11	16.75478	30.75478	0.0623709	4.1806631
6	17	29.205812	52.205812	0.0448158	9.2448633
8	9	24.165148	41.165148	0.0137623	1.9885941
24	37	85.076925	146.076925	0.0187861	33.520789
54	7	58.705402	119.705402	0.1350948	105.58106

Table 1: Some Values for the Parameters

The parameters e and E are from the theory of equations as follows. Since two of the roots form a complex conjugate pair, say $a \pm bi$, we can deduce from the sums of the roots one and two at a time that

$$y_0 = 2((b^2/3) + 2pq)^{\frac{1}{2}}. \tag{2.7}$$

For later generalization we re-write this as

$$y_0 = 2(2pq + e)^{\frac{1}{2}}, \tag{2.8}$$

and

$$y_0 = (E+2)(2pq)^{\frac{1}{2}}. \tag{2.9}$$

3. THE QUARTIC CASE

Ludovico Ferrari of Bologna (1522-1565), a student of Cardano, discovered the general method for solving quartics [6]. Consider now

$$x^4 = (x-p)^4 + (x-q)^4,\ p,q \in \mathbb{Z}_+, \tag{3.1}$$

which can be rewritten as

$$x^4 - 4(p+q)x^3 + 6(p^2+q^2)x^2 - 4(p^3+q^3)x + (p^4+q^4) = 0.$$

Now let

$$y = x - (p+q)$$

so that

$$y^4 - 12pqy^2 - 12pq(p+q)y - 2pq(2(p+q)^2 - pq) = 0. \tag{3.2}$$

Next consider the real valued function z defined by

$$z = y^4 - 12pqy^2 - 12pq(p+q)y - 2pq(2(p+q)^2 - pq). \tag{3.3}$$

Differentiation yields

$$\frac{dz}{dy} = 4y^3 - 24pqy - 12pq(p+q) \tag{3.4}$$

which at a stationary point of the curve (Figure 2) becomes the Cardano equation (2.2)

$$y^3 - 6pqy - 3pq(p+q) = 0. \tag{3.5}$$

At the point of inflection

$$\frac{d^2z}{dy^2} = 12y^2 - 24pq \tag{3.6}$$

and

$$y = \pm\sqrt{(2pq)}. \tag{3.7}$$

The gradients can be seen to be at their extremes where the curve crosses the y axis: nearly horizontal for negative y and approaching vertical for positive y. The roots of Equation (3.3) when $z = 0$ are two imaginary roots and

$$y_0 = -(2pq+d)^{\frac{1}{2}}, 3(2pq+e)^{\frac{1}{2}}.$$

Table 2 gives examples and Figure 2 shows that the negative roots are very close to the points of inflection.

p	q	d	e
2	3	0.234094	0.3265045
3	4	0.852977	0.56901

Table 2 : Examples for the Quartic

As can be seen, apart from $3(2pq+e)^{\frac{1}{2}}$, there is an additional real root $-(2pq+d)^{\frac{1}{2}}$. Two such forms for the real roots are found for all even n. The negative root may also be expressed by

$$y_0 = -(D+1)(2pq)^{\frac{1}{2}}$$

by comparison with (2.9) and with $D+1=(1+\frac{d}{2pq})^{\frac{1}{2}}$ and $d=2pqD(D+2)$.

4. THE QUINTIC CASE

Paolo Ruffini (1765-1822) anticipated the general idea of a group and claimed to have proved the insolvability of the quintic by radicals though it was Niels Henrik Abel (1802-1829) who finally settled the issue to the satisfaction of the mathematical community [6]. Consider

$$x^5=(x-p)^5+(x-q)^5,\ pq\in\mathbb{Z}_+, \tag{4.1}$$

which can be rewritten as

$$\begin{gathered}x^5-5(p+q)x^4+10(p^2+q^2)x^3-10(p^3+q^3)x^2\\+5(p^4+q^4)x-(p^5+q^5)=0.\end{gathered}$$

Now let

$$y=x-(p+q)$$

so that

$$\begin{gathered}y^5-20pqy^3-30pq(p+q)y^2-10pq(2(p+q)^2-pq)y\\-5pq(p+q)((p+q)^2-pq)=0.\end{gathered}$$

Next consider the real-valued function z defined by

$$\begin{gathered}z=y^5-20pqy^3-30pq(p+q)y^2-10pq(2(p+q)^2-pq)y\\-5pq(p+q)((p+q)^2-pq)\,.\end{gathered} \tag{4.2}$$

Differentiation yields

$$\frac{dz}{dy}=5y^4-60pqy^2-60pq(p+q)y-10pq(2(p+q)^2-pq) \tag{4.3}$$

so that stationary points occur when

$$y^4-12pqy^2-12pq(p+q)y-2pq(2(p+q)^2-pq)=0 \tag{4.4}$$

which is Equation (3.2). So too

$$\frac{d^2z}{dy^2}=20y^3-120pqy-60pq(p+q) \tag{4.5}$$

which at a point of inflection becomes the Cardano equation (2.2)

$$y^3 - 6pqy - 3pq(p+q) = 0. \tag{4.6}$$

Examples are shown in Figure 3 and Table 3.

p	q	x	e	E
2	3	19.0803408	0.3910001	0.0646443
3	4	26.8725894	0.6824871	0.0564752

Table 3: Examples for the Quintic

The one real root of Equation (4.2) with $z = 0$, is, as anticipated, given by $4(2pq + e)^{\frac{1}{2}}$.

5. THE GENERAL CASE

Consider now

$$x^n = (x-p)^n + (x-q)^n,$$

which, as a polynomial in x, has coefficients (Macmahon[9])

$$\begin{aligned}
\sum_{1\le i\le n} A_i &= n(p+q) \\
\sum_{1\le i<j\le n} A_iA_j &= \binom{n}{2}(p^2+q^2) \\
\sum_{1\le i<j<k\le n} A_iA_jA_k &= \binom{n}{3}(p^3+q^3) \\
&\cdots \\
A_1A_2A_3\ldots A_n &= p^n + q^n.
\end{aligned} \tag{5.1}$$

Then as before we can transpose to the form

$$z = (y+p)^n + (y+q)^n - (y+p+q)^n$$

then, following Gould [4] we have

$$z = y^n + \sum_{r=2}^{n}\binom{n}{r}(p^r + q^r - (p+q)^r)y^{n-r}$$

or

$$z = y^n - \sum_{r=2}^{n}\sum_{s=1}^{r-1}\binom{n}{r}\binom{r}{s}p^{r-s}\,q^s\,y^{n-r}. \tag{5.2}$$

If we differentiate with respect to y, we find that in general

$$\frac{d^m z}{dy^m} = n^m\{(y+p)^{n-m} + (y+q)^{n-m} - (y+p+q)^{n-m}\}$$

in which $n^{\underline{m}}$ is the falling factorial coefficient defined by

$$n^{\underline{m}} = n(n-1)...(n-m+1), \qquad m \in \mathbb{Z}_+,$$

so that

$$\frac{d^m z}{dy^m} = n^{\underline{m}} y^{n-m} - \sum_{r=2}^{n-m} \sum_{s=1}^{r-1} (n-r)^{\underline{m}} \binom{n}{r} \binom{r}{s} p^{r-s} q^s y^{n-r-m}$$

and for

$$\frac{d^{n-3} z}{dy^{n-3}} = 0$$

we have

$$0 = y^3 - \sum_{r=2}^{3} \sum_{s=1}^{r-1} (n-r)^{\underline{3}} \binom{n}{r} \binom{r}{s} p^{r-s} q^s y^{3-r},$$

that is,

$$0 = y^3 - 6pqy - 3pq(p+q)$$

which is the Cardano cubic equation. That the Cardano form of the cubic in Equation (2.2) has no integer roots can be seen here to be a consequence of Fermat's Last Theorem. The converse does not unfortunately hold since the Cardano cubic of the form

$$x^3 - 3rsx + (r^3 + s^3) = 0, \; r, s \in \mathbb{Z}_=,$$

always has at least one integer solution, $x = -(r+s)$. Not surprisingly with hindsight, Cardano cubics were involved in the proof of Fermat's Last Theorem in the form of elliptic curves (van der Poorten [12]). The graph of an elliptic curve is given by the points (x, y) of the equation

$$y^2 = x^3 + ax + b$$

in which $x, y, a, b, \in K$, where K is some field such that $4a^3 + 27b^2 \neq 0$ Galbraith [3] gives as examples of elliptic curves: $y^2 = x^3 - x$ over $\mathbb{R}$ and $y^2 = x^3 + 3x + 7$ over $\mathbf{F}_{17}$, the finite field of integers modulo a prime $p > 3$. In the latter case $4a^3 + 27b^2 \neq 0 (mod 17)$. More formally, the elliptic curve is defined to be the set

$$E = \{(x, y) : x, y \in K \; \wedge y^2 = x^3 + ax + b\} \cup \{O_E\}$$

in which O_E is the "point at infinity".

For $z = 0$ and n odd in Equation (5.2) we always obtain a set of complex roots and their conjugates and one real non-integer root given by

$$y_0 = (n-1)(2pq + e)^{\frac{1}{2}}. \tag{5.3}$$

For n even there are two real non-integer roots, one in the form given in Equation (5.3) and one given by

$$y_0 = -(2pq + d)^{\frac{1}{2}}. \tag{5.4}$$

Some examples of e, E, d, D as functions of n are shown in Table 3.

p	q	n	E	e	D	d
2	3	2	0	0	0	0
		3	0.0181208	0.2184349		
		4	0.0405392	0.3265045	0.0097068	0.234094
		5	0.064644	0.3909984		
		6	0.0895845	0.4338579	0.0103139	0.24881
		7	0.1149973	0.4643973		
		9	0.1663886	0.5043568		
3	4	2	0	0	0	0
		3	0.0157567	0.3796493		
		4	0.0353548	0.56901	0.0176152	0.852977
		5	0.0564752	0.6824871		
		6	0.077*	0.74489*		
		7	0.098*	0.79040*		
		8	0.1187*	0.82084*		
		9	0.139*	0.84125*		

Table 3: Parameter Values; * estimates from E vs n line

The parameter E is linear in n for the range $n = 3, 4, ..., 9$. This permits y_0 to be estimated. If we assume that the linearity holds at $n = 100$, then $E = 2.274496$ for the $< p, q >$ set $< 2, 3 >$ and $e = 0.55773$ compared with $e = 0.504357$ at $n = 9$.

On the other hand the e versus n curve flattens very rapidly and approaches a constant non-integer value for e. Furthermore, for $n = 3$, e versus p/q, $p < q$, yields a rectangular hyperbola, with the value of e increasing rapidly when $p << q$. The characteristics of these parameters explain the persistence of the non-integer status of y_0. For $n = 3$, e has the form

$$64e^3 + 64(3pq)e^2 + 144(pq)^2 e + 32(pq)^3 - 9(pq)^2(p+q)^2 = 0$$

which yields one real non-integer value for e and a complex conjugate pair. Analogous equations can be found for higher n.

6. CONCLUSION

At this stage what one would like are conveniently obtained approximate solutions of Equation (5.2) which by the Harriot-Descartes Rule of Signs [11] cannot have more than one positive root. To do this we modify Bernoulli's iteration [7]. In doing so we respond to the speculation of de Pillis [10] about the generalisation of his observations on Newton's formula for finding the root of a non-linear function when applied to cubic polynomials.

The following outline is in the spirit of Cardano who was motivated to find approximate solutions of polynomial equations [5].

With Bernoulli's method for finding the dominant zero of $f(y)$ of degree n, one has simply to calculate $f(n), f(n+1), f(n+2)$, giving $f(0), f(1), f(2), \ldots, f(n-1)$ any set of values, but preferably $1, \xi, \xi^2, \ldots, \xi^{n-1}$, and then take $f(y+1)/f(y)$ as an approximation to the dominant zero. For notational convenience we re-write Equation (5.2), $z = 0$, as

$$y^n = \sum_{j=1}^{n} P_j y^{n-j}. \tag{6.1}$$

Then

$$y^{n+r} = \sum_{j=0}^{n-1} Q_{r,j} y^j, \tag{6.2}$$

where

$$Q_{r,0} = P_n u_r \text{ and } Q_{o,m} = P_{n-m},$$

$$Q_{r,m} = \begin{cases} 0, & m \geq n, m < 0, n < 0, \\ Q_{r-1,m-1} + P_{n-m} Q_{r-1,n-1}, & 0 < m < n, \end{cases}$$

and

$$u_r = \sum_{j=1}^{n} P_j u_{r-j}, \; n > 0,$$

with $u_r = 0$, $n < 0$, and $u_0 = 1$. Some examples of $Q_{r,m}$ are given in Table 4.

$m =$	0	1	0	1	2	0	1	2	3
$r = 0$	1	1	1	1	1	1	1	1	1
1	1	2	1	2	1	1	2	2	1
2	2	3	1	2	3	1	2	3	1
3	3	5	3	4	5	1	2	3	4
4	5	8	5	8	9	4	5	6	7
5	8	13	9	14	17	7	11	12	13
6	13	21	17	26	31	13	20	24	25
7	21	34	31	48	57	25	38	45	49
n	2	2	3	3	3	4	4	4	4

Table 4: $Q_{r,m}$ for n=2,3,4 and P_j=1

Proof of (6.2): We use induction on r. For $r = 0$,

$$\sum_{j=0}^{n-1} Q_{0,j} y_j = \sum_{j=0}^{n-1} P_{n-j} y^j = y^{n+0}.$$

Assume the result is true for $r = 1, 2, 3, \ldots, s$.

$$y^{n+s+1} = \sum_{j=0}^{n-1} Q_{s,j}\, y^{j+1}$$

$$= Q_{s,n-1} y^n + \sum_{j=0}^{n-2} Q_{s,j}\, y^{j+1}$$

$$= Q_{s,n-1} y^n + \sum_{j=0}^{n-1} Q_{s,j-1}\, y^j$$

$$= Q_{s,n-1} y^n + \sum_{j=0}^{n-1} Q_{s+1,j-1}\, y^j - \sum_{j=0}^{n-1} P_{n-j} Q_{s,n-1} y^j$$

$$= Q_{s,n-1} y^n - Q_{s,n-1} \sum_{j=0}^{n-1} P_{n-j}\, y^j + \sum_{j=0}^{n-s} Q_{s+1,j-1}\, y^j$$

$$= \sum_{j=0}^{n-1} Q_{s+1,j}\, y^j, \qquad \text{as required.}$$

For example, consider the Cardano cubic

$$y^3 = y + 1.$$

From Table 4 we have

$$y^5 = y^2 + y + 1$$

and

$$y^6 = y^2 + 2y + 1$$

and Bernoulli's iteration would give y^6/y^5 as an approximation to the dominant root α. Result (6.2) enables us to accelerate the iteration and speed up the convergence to yield

$$y^{48} = 170625y^2 + 226030y + 128801$$

and

$$y^{49} = 226030y^2 + 299426y + 170624,$$

so that

$$\alpha = \begin{cases} 1.324717957 & \text{when } y = 1, \\ 1.324717955 & \text{when } y = 2, \\ 1.324717973 & \text{when } y = 1.3. \end{cases}$$

This enables us to find the dominant root quickly. The presence of a non-integer root does not mean that there are no integer roots, except in the cases covered by Fermat's Last Theorem.

```
In[34]:= f[p_, q_, y_] = y^3 - 6*p*q*y - 3*p*q*(p + q)

Out[34]= -3 p q (p + q) - 6 p q y + y^3

In[41]:= a = Plot[f[2, 3, y], {y, -14, 14}, PlotRange -> {-700, 800}]
         b = Plot[f[3, 4, y], {y, -14, 14}, PlotRange -> {-700, 800}]
         Show[a, b]
```

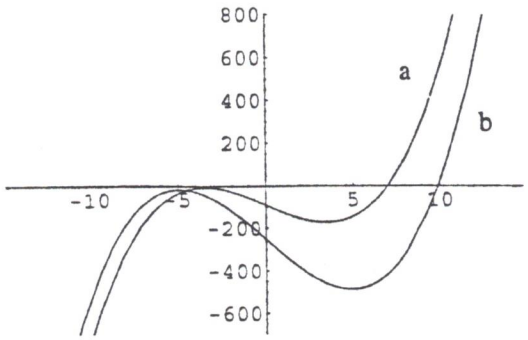

Figure 1

```
Out[43]= - Graphics -

In[44]:= f[p_, q_, y_] = y^4 - 12*p*q*y^2 - 12*p*q*(p + q)*y + 2*p*q*(p*q - 2*(p + q)^2)

Out[44]= 2 p q (p q - 2 (p + q)^2) - 12 p q (p + q) y - 12 p q y^2 + y^4

In[48]:= c = Plot[f[2, 3, y], {y, -15, 16}, PlotRange -> {-20000, 10000}]
         d = Plot[f[3, 4, y], {y, -15, 16}, PlotRange -> {-20000, 10000}]

         Show[c, d]
```

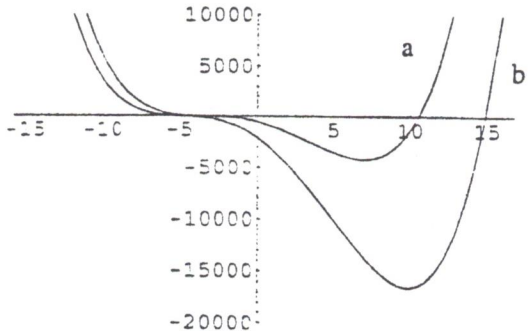

Figure 2

```
Out[50]= - Graphics -

In[22]:= f[p_, q_, y_] = y^5 - 20*p*q*y^3 - 30*p*q*(p + q)*y^2 +
           10*p*q*(p*q - 2*(p + q)^2)*y - 5*p*q*(p + q)*((p + q)^2 - p*q)
         a = Plot[f[2, 3, y], {y, -20, 24}, PlotRange -> {-900000, 400000}]
         b = Plot[f[3, 4, y], {y, -20, 24}, PlotRange -> {-900000, 400000}]

         Show[a, b]
```

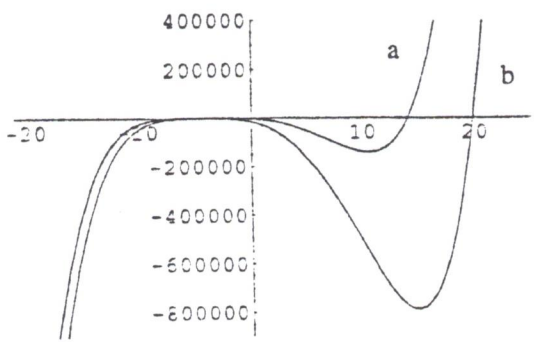

Figure 3

```
Out[25]= - Graphics -
```

REFERENCES

1. Boyer, Carl B. 1985. *A History of Mathematics*. Princeton: Princeton University Press.

2. Dunham, William. 1990. *Journey through Genius: The Great Theorems of Mathematics*. New York: John Wiley.

3. Galbraith, Steven. 1999. Elliptic Curve Public Key Cryptography. *Mathematics Today*. 35(3): 76-79.

4. Gould, Henry W. 1999. The Girard – Waring Power Sum Formulas for Symmetric Functions and Fibonacci Sequences. *The Fibonacci Quarterly*. 37(2): 135-140.

5. Herz-Fischler, Roger. 1998. *A Mathematical History of the Golden Section*. New York: Dover.

6. Hillman, Abraham P. & Alexanderson, Gerald L. 1978. *A First Undergraduate Course in Abstract Algebra*. Second Edition. Belmont, CA: Wadsworth.

7. Householder, A.S. 1970. *The Numerical Treatment of a Single Non-linear Equation*. New York: McGraw-Hill.

8. McLeish, John. 1991. *The Story of Numbers*. New York: Fawcett Columbine.

9. Macmahon, Percy A. 1915. *Combinatory Analysis*. Volume I. Cambridge: Cambridge University Press.

10. de Pillis, L.G. 1998. Newton's Cubic Roots. *The Australian Mathematical Society Gazette*. 25(5): 236-241.

11. Turnbull, H.W. 1952. *Theory of Equations*. Fifth Edition. Edinburgh: Oliver and Boyd.

12. van der Poorten, A. 1996. *Notes on Fermat's Last Theorem*. New York: Wiley.

AMS Classification Numbers: 11C08, 11D41