INFORMATION TO USERS

This reproduction was made from a copy of a document sent to us for microfilming. While the most advanced technology has been used to photograph and reproduce this document, the quality of the reproduction is heavily dependent upon the quality of the material submitted.

The following explanation of techniques is provided to help clarify markings or notations which may appear on this reproduction.

1. The sign or "target" for pages apparently lacking from the document photographed is "Missing Page(s)". If it was possible to obtain the missing page(s) or section, they are spliced into the film along with adjacent pages. This may have necessitated cutting through an image and duplicating adjacent pages to assure complete continuity.

2. When an image on the film is obliterated with a round black mark, it is an indication of either blurred copy because of movement during exposure, duplicate copy, or copyrighted materials that should not have been filmed. For blurred pages, a good image of the page can be found in the adjacent frame. If copyrighted materials were deleted, a target note will appear listing the pages in the adjacent frame.

3. When a map, drawing or chart, etc., is part of the material being photographed, a definite method of "sectioning" the material has been followed. It is customary to begin filming at the upper left hand corner of a large sheet and to continue from left to right in equal sections with small overlaps. If necessary, sectioning is continued again beginning below the first row and continuing on until complete.

4. For illustrations that cannot be satisfactorily reproduced by xerographic means, photographic prints can be purchased at additional cost and inserted into your xerographic copy. These prints are available upon request from the Dissertations Customer Services Department.

5. Some pages in any document may have indistinct print. In all cases the best available copy has been filmed.

University Microfilms International
300 N. Zeeb Road
Ann Arbor, MI 48106

Wajngurt, Clara

SOLUTIONS OF DIOPHANTINE EQUATIONS OVER C(T) AND COMPLEX MULTIPLICATION

City University of New York PH.D. 1983

PLEASE NOTE:

In all cases this material has been filmed in the best possible way from the available copy. Problems encountered with this document have been identified here with a check mark ✓.

1. Glossy photographs or pages _____
2. Colored illustrations, paper or print _____
3. Photographs with dark background _____
4. Illustrations are poor copy _____
5. Pages with black marks, not original copy ✓
6. Print shows through as there is text on both sides of page _____
7. Indistinct, broken or small print on several pages ✓
8. Print exceeds margin requirements _____
9. Tightly bound copy with print lost in spine _____
10. Computer printout pages with indistinct print _____
11. Page(s) _____ lacking when material received, and not available from school or author.
12. Page(s) _____ seem to be missing in numbering only as text follows.
13. Two pages numbered _____. Text follows.
14. Curling and wrinkled pages _____
15. Other _____

University
Microfilms
International

SOLUTIONS OF DIOPHANTINE EQUATIONS OVER $\mathbb{C}(t)$ AND COMPLEX MULTIPLICATION

by

Clara Wajngurt

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York.

1983

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

February 18, 1983
Date

Harvey Cohn
Chairman of the Examining Committee
Professor Harvey Cohn

February 18, 1983
Date

Executive Officer
Professor Alex Heller

Professor Alphonse T. Vasquez

Professor Raymond Hoobler

Supervisory Committee

The City University of New York

Abstract

Solutions of Diophantine Equations over $\mathbb{C}(t)$

and Complex Multiplication

by

Clara Wajngurt

Advisor: Professor Harvey Cohn

In this paper we establish a relationship between the rational solutions $(x(t),y(t))$, over $\mathbb{C}(t)$, of the diophantine equation:

$$4t^3x(t)^3-g_2tx(t)-g_3 = y(t)^2(4t^3-g_2t-g_3),\ g_2,g_3 \in \mathbb{C} \quad (1)$$

and the solutions $(p(u),p'(u))$ which parametrize the elliptic curve $E:y^2 = 4x^3-g_2x-g_3$ admitting complex multiplication by λ. E is identified with the group $\mathbb{C}/L$ whereby L is a lattice which is generated by the periods $2\omega_1$, $2\omega_2$, with $\mathrm{Im}(\omega_1/\omega_2) > 0$. By definition of complex multiplication by λ, we are interested in those multipliers, $\lambda \in C$ for which $\lambda L \subset L$. According to the theory, all such multipliers λ belong to the ring of integers of some imaginary quadratic field K. In particular we restrict our theory to $g_2,g_3 \in \mathbb{Q}$ so that the problem which is discussed here is fully solved for the case of K, having ring class number one. As a result the paper attempts to expand on the work of H. Cohn who dealt with the two specific diophantine equations over $\mathbb{C}(t)$, which had specific values for g_2,g_3 and which corresponded to the two cases $K = \mathbb{Q}(\sqrt{-1})$, $(t = 4p^2(u))$ and $K = \mathbb{Q}(\sqrt{-3})(t = 4p^3(u))$. Concluding remarks about solving the problem for K having ring class number greater than one are made.

The basic results of this paper are consequences of results in elliptic function theory having to do with elliptic integrals of the first kind. We first characterize the form of all rational solutions of diophantine equation (1). The rational solutions are derivable from the substitutions

$$x(t) = \frac{p(\lambda u+\mu)}{p(u)} \qquad y(t) = \frac{p'(\lambda u+\mu)}{p'(u)} \qquad t = p(u)$$

in which $\mu = 0, \omega_1, \omega_2, \omega_1 + \omega_2$. As a corollary we show through a minor change in notation, a relationship between the modular invariants of diophantine equation (1) in modified form, and the elliptic curve E, admitting complex multiplication by λ. Using techniques established in elliptic function theory, we prove that the complex multiplier λ, associated with a unique rational solution $(x(t),y(t))$, must be of a certain form. Next, we construct all rational solutions of diophantine equation (1) by using the addition theorems valid for the Weierstrass function, $p(u)$. When both λ,μ are non-zero, we use the expression:

$$p(u+\omega_i) = \frac{e_i p(u) + (2e_i^2-(1/4)g_2)}{p(u)-e_i} \qquad e_i = p(\omega_i),$$

to find the associated rational solution $(x(t),y(t))$. Specific examples are worked out for the cases $K = \mathbb{Q}(\sqrt{-2})$ and $K = \mathbb{Q}(\sqrt{-1})$. Actual applications to each of the thirteen diophantine equations with specific g_2,g_3, and corresponding respectively to the thirteen imaginary quadratic rings, having class number one, are made. Finally, we analyze for all possible cases the smallest field of containment for the rational solutions $(x(t),y(t))$ of diophantine equation (1).

Since there is an expression which explicitly describes the Weierstrass elliptic function $p(u)$ in terms of the Jacobian elliptic function $sn(u;k)$ (k = modulus); in conclusion, we wonder, as a point for future investigative study, as to whether the ensuing theory resting on results of Weierstrass elliptic functions can be applied in some modified form to Jacobian elliptic functions as well.

Acknowledgements

There are several people I must thank for helping me reach the stage I have achieved at this present day. For, it is without them that I would never have accomplished this achievement. First, I would like to thank my advisor, Dr. Cohn not only for the encouragement, patience, and time he gave me during the preparation of this thesis, but for his perceptiveness, in determining a topic that coincides with my mathematical needs, and that captivated my interest, right from the start. It is often that I have heard of students not being genuinely interested in a topic that has previously been selected for them. It is with this genuine interest, motivated by my adviser, that I have learned to be mathematically more confident and mature. Secondly, I must thank my mother, and my father (ז"ל), who always wanted my brother and I to achieve a good education. For rooted in the deep traditional values of Judaism, I was not only taught tolerance of others and a sense of rationality but a determination to strive for specific goals. This sense of tolerance and rationality has consistently helped me in logical reasoning so necessary in understanding and performing mathematics. Thus, it is with pride that I, an offspring of parents who grew up in Kostopol, a town in eastern Poland (province of Wolyn), and who survived an inconceivable Holocaust, can share with others the knowledge I have learned in this paper.

TABLE OF CONTENTS

List of Tables Page

Section 1: Background

Given the diophantine equation

$$4t^3x(t)^3 - g_2tx(t) - g_3 = y(t)^2(4t^3-g_2t-g_3) \qquad (1)$$
$$g_2, g_3 \in \mathbb{Q}$$

where $x(t)$, $y(t)$ are rational functions in $\mathbb{C}(t)$.
We would like to characterize all rational solutions $x(t)$, $y(t) \in \mathbb{C}(t)$ satisfying this diophantine equation. The following discussion will clarify the two cases:

(1) deg $x(t)$ = deg $y(t)$

(2) deg $x(t) \neq$ deg $y(t)$

Our results will be discussed shortly.

1.1: The meaning of complex multiplication

Any elliptic curve, E, is identified with the group $\mathbb{C}/L$ where L is generated by the periods $2\omega_1$, $2\omega_2$, with $\mathrm{Im}(\omega_1/\omega_2) > 0$. The complex analytic endomorphisms of the lattice L which preserve the elliptic curve E, $\alpha(x) = \lambda x$, $\lambda \in \mathbb{C}$, $x \in L$ are identified with the multiplication by a complex number, λ, such that $2\omega_1\lambda$, $2\omega_2\lambda \in L$. These endomorphisms of the lattice form a ring which always contain the integers, i.e., $\lambda \in \mathbb{Z}$ - the real multiplications. The other complex analytic endomorphisms (if any) are given by complex numbers and are called complex multiplications. Although the real multiplications are a subset of the complex multiplications, we say the elliptic curve admits complex multiplications, only when the endomorphism ring of E (or endomorphism ring of $\mathbb{C}/L$) corresponds to the multiplication of complex numbers λ, $\lambda \notin \mathbb{Z}$. The theory shows that all complex multipliers λ, belonging to End E (i.e.,

the corresponding elliptic curve to lattice L admits the complex multiplications, λ_ζ) belong to the ring of integers, θ_K of some imaginary quadratic field, $K = \mathbb{Q}(\sqrt{d})$ ($d < 0$, d square free). The generating basis for θ_K is given by $[1,\omega]$ where

$$\omega = \begin{cases} \sqrt{d} & d \not\equiv 1 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & d \equiv 1 \pmod 4 \end{cases}$$

In particular End $E \tilde{=} \mathbb{Z} + f\theta_K \tilde{=} [1,f\omega] = \theta_f$ where f = ring conductor of End E.

1.2: Why we restrict ourselves to $g_2, g_3 \in \mathbb{Q}$

Let L be the lattice $[2\omega_1, 2\omega_2]$ and $\mathbb{C}/L$ the compact Riemann surface of genus one, described earlier. An elliptic function with periods in L is a meromorphic function on $\mathbb{C}$ which is invariant under the translation: $u \mapsto u + \omega$ where $\omega = 2a\omega_1 + 2b\omega_2$ $a,b \in \mathbb{Z}$. Define complex numbers g_2, g_3 and meromorphic functions $\wp(u)$ and $\wp'(u)$ on $\mathbb{C}$ by

$$g_2 = g_2(L) = 60\Sigma\omega^{-4}$$
$$g_3 = g_3(L) = 140\Sigma\omega^{-6}$$
$$\wp(u) = \wp(u;L) = u^{-2} + \Sigma\{(u-\omega)^{-2} - \omega^{-2}\}$$
$$\wp'(u) = \wp'(u;L) = -2\Sigma(u-\omega)^{-3}$$

where each of the above sums, Σ, are taken over all non-zero ω in L. By elliptic function theory we find that

$$\wp_L'(u)^2 = 4\wp_L(u)^3 - g_2\wp_L(u) - g_3, \quad g_2^3 - 27g_3^2 \neq 0.$$

In addition, the field of all elliptic functions with periods in L is the same as $\mathbb{C}(\wp_L(u), \wp_L'(u))$, the field over $\mathbb{C}$, generated by $\wp_L(u)$ and $\wp_L'(u)$.

Let E be the algebraic curve with a "zero" point (∞,∞), given by $(X,Y) \in \mathbb{C}$ such that:

$$y^2 = 4X^3 - g_2X - g_3 \qquad g_2^3 - 27g_3^2 \neq 0$$

$$y = p'(u) \qquad X = p(u)$$

The map $u \in \mathbb{C} \longmapsto (p(u), p'(u)) \in E$, referred to earlier, describes the isomorphism of $\mathbb{C}/L$ onto E; E is viewed as a complex manifold, with differential dx/y, which pulls back to the differential du, on C. Any elliptic curve $y^2 = 4X^3 - g_2X - g_3$, $g_2^3 - 27g_3^2 \neq 0$ is identified with a modular invariant $j_L = j(\omega_1/\omega_2)$, a number which depends on the lattice L, $\mathrm{Im}(\omega_1/\omega_2) > 0$, namely

$$j_L = 2^6 \cdot 3^3 \cdot \frac{g_2^3}{g_2^3 - 27g_3^2}$$

where g_2, g_3 are the previously defined complex numbers depending on the lattice, L.

On the other hand, given any value for j_L, one can always find an elliptic curve with invariant j_L, namely

$$Y^2 = 4X^3 - cX - c \qquad c = g_2 = g_3$$

with

$$j_L = 2^6 \cdot 3^3 \cdot \frac{c^3}{c^3 - 27c^2} = 2^6 \cdot 3^3 \cdot \frac{c}{c-27}$$

which when solved for c:

$$c = \frac{27j_L}{j_L - 2^6 \cdot 3^3}.$$

For the two special cases, $j_L = 0$, $j_L = 2^6 \cdot 3^3$, we associate the curves

$$Y^2 = 4X^3 - 1 \qquad \text{with} \qquad j_L = 0$$

and

$$Y^2 = 4X^3 - X \qquad \text{with} \qquad j_L = 2^6 \cdot 3^3.$$

This shows that $g_2, g_3 \in \Phi \rightarrow j_L \in \Phi$.

Therefore, why do we restrict our discussion in this paper to $j_L \in \Phi$?

We recall that

End E = ring of endomorphisms of lattice L which preserve the elliptic curve E and keep the "zero" point of E, fixed.

$$L = [2\omega_1, 2\omega_2] \qquad \mathrm{Im}(\omega_1/\omega_2) > 0.$$

In general, End $E \cong \mathbb{Z}$, unless $K = \Phi(\omega_1/\omega_2)$ $(= \mathbb{Q}(\lambda)$, when λ is a complex multiplier) is an imaginary quadratic field. So $K = \Phi(\omega_1/\omega_2)$ is an imaginary quadratic field, if the elliptic curve E admits complex multiplications. According to the theory, $j_L = j(\omega_1/\omega_2)$ is an algebraic integer, if E admits complex multiplications. This means $[\mathbb{Q}(j_L): \Phi] < \infty$, for by Siegel's theorem (see [2], pg. I-3) if ω_1/ω_2 is an algebraic integer in the upper half-plane <u>not</u> belonging to a quadratic imaginary field, then $j(\omega_1/\omega_2)$ is transcendental. Especially, by the theory the degree $[\mathbb{Q}(j_L): \Phi] \leq h_f$ where f = ring conductor of End E and h = ring class number of $K = \Phi(\omega_1/\omega_2)$. The degree of j_L over Φ equals the class number, h, when f = 1. When $j_L \in \Phi$, i.e., when $g_2, g_3 \in \Phi$, the class number h_f of the corresponding imaginary quadratic field K is one, for $f \geq 1$. Therefore, why do we restrict our discussion in this paper to a $K = \Phi(\omega_1/\omega_2)$ (which contains the ring of complex multipliers for our curve, E) having class number one, $f \geq 1$? Assume $h_f > 1$, i.e., $j_L \notin \Phi$. By the theory, the elliptic curves E admitting complex multiplication, and having <u>given</u> endomorphism

ring θ_f = End E are in one to one correspondence with the class group of θ_f, $\theta_f = \mathbb{Z} + f\theta_K$. This means that to each element of the class group of θ_f, there corresponds a unique elliptic curve; each of these elliptic curves has the same ring of endomorphisms, θ_f. On the other hand, given the endomorphism ring θ_f ($f \geq 1$), there are finitely many elliptic curves-precisely, the theory shows that there are

$$h_f = |\text{class group of } \theta_f|$$

= ring class number of the imaginary quadratic field, K, such elliptic curves. As an example, when f = 1, the class group of θ_f is merely the group of ideal classes of θ_K. Let us restrict this discussion to the case f = 1, class number $h > 1$ and analyze the consequences. In this case we have for each elliptic curve E_i, θ_f = End E_i = θ_K = <u>full</u> ring of integers of the imaginary quadratic field K, $1 \leq i \leq h$. By definition, E_1, is <u>isogenous</u> to E_2, if the lattice L_1 corresponding to the curve E_1 is related to the lattice L_2, corresponding to the curve E_2, only when there exists an $\alpha \in K$ with $\alpha L_1 \subset L_2$. We claim that in our case, f = 1, $h_f > 1$; $E_1, E_2, \ldots, E_h$ is a full equivalence class of isogenic curves, if the respective lattices, $L_1, L_2, \ldots, L_h$, to each of the elliptic curves E_i ($1 \leq i \leq h$) are contained in the imaginary quadratic field, K. Applying this definition as follows, we suppose End E_1 = End E_2. Without loss of generality, assume also $L_1 = [1, \tau]$, $L_2 = [1, \tau']$ where $\tau = \omega_1/\omega_2$, $\tau' = \omega_1'/\omega_2'$ are both imaginary quadratic numbers with a positive imaginary part. Assume $\tau, \tau' \in K = \mathbb{Q}(\omega_1/\omega_2)$. Then E_1 is isogenous to E_2. This is the case, because

$\tau = a\tau' + b$, for $a > 0$ ($Im(\tau) > 0$), $b \in \Phi$ implies $1 \cdot L_1 \subset L_2$; which means that any complex multiplier $\alpha \in \theta_K$ satisfies $\alpha \cdot L_1 \subset L_1 \subset L_2$. A similar argument shows E_2 is isogenous to E_1. (In particular, the set of elliptic curves E_i with θ_f = End $E_i = \theta_K$ is a full equivalence class of isogenic curves). This means there exists a correspondence in which any E_i, $1 \leq i \leq h$; h = cardinality of the class group θ_f; in the set, is isogenous to any selected E_j, $1 \leq j \leq h$. The following theory produces a correspondence between diophantine equation (1) and the elliptic curve E; $y^2 = 4x^3 - g_2x - g_3$. If $h > 1$, i.e., $g_2, g_3 \notin \Phi$, the following theory will show that perhaps more than one elliptic curve E (all isogenous, however, but not necessarily isomorphic) would be associated with diophantine equation (1). Thus, we are interested in associating diophantine equation (1) with one, unique curve E. This means we want this elliptic curve E to admit complex multiplications that belong to the ring of integers of some imaginary quadratic field K, having class number one. In the case of class number one there are thirteen corresponding elliptic curves which do indeed have $g_2, g_3 \in \Phi$. These thirteen elliptic curves defined over Φ, will be explicitly outlined later.

Section 2: Discussion

Recall the elliptic curve

$$\eta^2 = 4\xi^3 - g_2\xi - g_3 \qquad g_2^3 - 27g_3^2 \neq 0 \qquad g_2, g_3 \in \Phi$$

is solvable by Weierstrass elliptic functions contained in the elliptic function field, $\Phi(p_L(u), p_L'(u))$ $L = [2\omega_1, 2\omega_2]$, namely,

$$\xi = p(u) \qquad \eta = p'(u) \tag{2}$$

and u, a variable in $\Phi(p_L(u), p_L'(u))$. This curve generates a Riemann surface on which the differential of the first kind $d(p(u))/p'(u) = du$ is defined.

2.1: Basic form of all rational solutions $(x(t), y(t))$

Let $(x(t), y(t))$ be a solution of diophantine equation (1). Set A(u), B(u) as follows:

$$A(u) = x(p(u))p(u) \qquad B(u) = y(p(u))p'(u) \tag{3}$$

where $x(p(u)), y(p(u)) \in$ Rat functions $\{p(u)\}$. Since $x(p(u))$, $y(p(u))$ are both rational functions in $p(u)$ we can set $p(u) = t$ in the functions $x(p(u))$, $y(p(u))$, thereby obtaining rational functions in t.

In (1) we substitute for $(x(t), y(t))$

$$\frac{A(u)}{p(u)} = x(t) \qquad \frac{B(u)}{p'(u)} = y(t) \qquad t = p(u) \tag{3'}$$

to obtain

$$4p^3(u)\,\frac{A^3(u)}{p^3(u)} - g_2 p(u)\,\frac{A(u)}{p(u)} - g_3 =$$

$$\frac{B^2(u)}{p'^2(u)}\,\{4p^3(u) - g_2 p(u) - g_3\}.$$

By cancellation and statement (2) we produce the elliptic curve

$$4A^3(u) - g_2A(u) - g_3 = B^2(u) \qquad (4)$$
$$g_2^3 - 27g_3^2 \neq 0 \qquad j_L \in \Phi$$

which is associated with the unique differential of the first kind $d(A(u))/B(u)$. By elliptic function theory

$$A(u) = p(\omega) \qquad B(u) = p'(\omega)$$

for some variable ω, to be determined later. Since the dimension of the space of holomorphic differentials on a compact Riemann surface of genus one, equals one, we find

$$\frac{d(A(u))}{B(u)} = d\omega = \lambda du \qquad (4')$$

for some $\lambda \in \mathbb{C}^*$. This implies $\omega = \lambda u + \mu$, μ determined modulo the lattice $[2\omega_1, 2\omega_2]$ associated with $p(u)$.
Therefore

$$A(u) = p(\lambda u+\mu)$$
$$B(u) = p'(\lambda u+\mu) \qquad (5)$$

In particular we note that by statement (3) and the symmetry of the elliptic function $p(u)$

$$A(-u) = A(u).$$

With statement (5), this means

$$p(\lambda u+\mu) = p(\lambda(-u)+\mu) = p(-\lambda u+\mu)$$

and then either

$$\lambda u + \mu \equiv -\lambda u + \mu \bmod\{2\omega_1, 2\omega_2\}, \text{ impossible}$$

or

$$\lambda u + \mu \equiv -(-\lambda u+\mu) \bmod\{2\omega_1, 2\omega_2\}$$

$$\Leftrightarrow \qquad \mu \equiv -\mu \qquad \mod\{2\omega_1, 2\omega_2\}$$

$$\Leftrightarrow \qquad 2\mu \equiv 0 \qquad \mod\{2\omega_1, 2\omega_2\}$$

Therefore statement (5) becomes

$$\begin{aligned} A(u) &= \wp(\lambda u+\mu) \\ B(u) &= \wp'(\lambda u+\mu) \end{aligned} \tag{5'}$$

with the conditions $\mu = 0, \omega_1, \omega_2, \omega_1 + \omega_2 = \omega_3$.

This leads us to the following conclusion:

Theorem 1: We can derive infinitely many solutions $(x(t), y(t)) \in \mathbb{C}(t)$ satisfying diophantine equation (1), only by way of the substitutions

$$x(t) = \frac{\wp(\lambda u+\mu)}{\wp(u)} \qquad y(t) = \frac{\wp'(\lambda u+\mu)}{\wp'(u)}, \qquad t = \wp(u).$$

In the process, we consider that

$$X = \wp(u) \qquad Y = \wp'(u)$$

parametrize $Y^2 = 4X^3 - g_2X - g_3$, $g_2^3 - 27g_3^2 \neq 0$; $g_2, g_3 \in \mathbb{C}$ and $\mu = 0, \omega_1, \omega_2, \omega_1 + \omega_2$.

Remark 1

Statements (3), (3') and (5') are necessary conditions for deriving rational solutions of diophantine equation (1). In effect, we will observe that all rational solutions correspond to complex (cr real) multipliers, λ. By the following lemma we claim they are sufficient conditions also, for deriving solutions of diophantine equation (1).

Lemma 1. If λ is a complex (or real) multiplier, $2\mu \equiv 0 \mod \{2\omega_1, 2\omega_2\}$ then $\wp(\lambda u+\mu)$ is a rational function in $\wp(u)$.

Proof. Suppose $p(u)$ has real period $2\omega_1$ and complex period $2\omega_2$. Let $\lambda = m + n\tau \quad m,n \in \mathbb{Z};\ \tau \in \mathbb{C}$ where $\lambda \in$ ring of endomorphisms of the given lattice. We are assuming that the lattice L corresponding to $p(u)$ admits complex multiplication by λ. This implies

$$p(u+2\omega_1) = p(u)$$
$$p(u+2\omega_2) = p(u).$$

Then

(1) $p(\lambda(u+2\omega_1)) = p(\lambda u+\lambda\cdot 2\omega_1) = p(\lambda u),\ \lambda\cdot 2\omega_1 \subset L$

(11) $p(\lambda(u+2\omega_2)) = p(\lambda u+\lambda\cdot 2\omega_2) = p(\lambda u),\ \lambda\cdot 2\omega_2 \subset L$

By

(1) $p(\lambda u+2\omega_1) = p(\lambda u)$

(11) $p(\lambda u+2\omega_2) = p(\lambda u)$

Therefore, any period of $p(u)$ will be a period of $p(\lambda u)$, when λ is a complex (or real) multiplier. In addition, any period of $p(u)$ is a period of $p(\lambda u+\mu)$; especially when $\mu = 0,\ \omega_1,\ \omega_2,\ \omega_1 + \omega_2$. This means that the quotient $p(\lambda u+\mu)/p(u)$ is an elliptic function with the same period lattice as $p(u)$. Keeping in mind $2\mu \equiv 0 \bmod\{2\omega_1, 2\omega_2\}$ and $p(-u) = p(u)$, we have that $p(\lambda u+\mu)/p(u)$ is an even elliptic function, and is thereby expressible as a rational function, having complex coefficients, of the function $p(u)$, with the same period lattice as $p(u)$. Thus $p(\lambda u+\mu)$ is a rational function in $p(u)$.

Remark 2

The above statements motivate the following conclusions: Every rational solution $(x(t),y(t))$ of diophantine equation (1) is

intrinsically of the given form described by statements (3') and (5') if and only if λ is a complex (or real) multiplier. Before we outline an explicit method for constructing any rational solution, let us consider the following corollary implied by the above statements:

Corollary 1. Let the curves C_1 and C_2 be defined as follows:

$$C_1: B^2 = 4A^3 - g_2A - g_3$$
$$C_2: 4t^3X^3 - g_2tX - g_3 = Y^2(4t^3-g_2t-g_3)$$
$$g_2^3 - 27g_3^2 \neq 0 \qquad g_2, g_3 \in \mathbb{Q}$$

For those complex values of t for which C_2 is an elliptic curve having genus one (e.g., t = 0, excluded), the curves C_1 and C_2 have the same modular invariants. In this case, by the theory, C_1 and C_2, both viewed over $\mathbb{C}$, are isomorphic.

Proof. The modular invariant, j of C_1 is $2^6 \cdot 3^3 \cdot \dfrac{g_2^3}{g_2^3-27g_3^2}$.

We are to show that C_2, when viewed as an elliptic curve has the same modular invariant as C_1; t is a fixed complex number. We write C_2 in the form $y^2 = f(x)$.

$$4\left\{\frac{t^3}{4t^3-g_2t-g_3}\right\}X^3 - \left\{\frac{t}{4t^3-g_2t-g_3}\right\}g_2X - \left\{\frac{g_3}{4t^3-g_2t-g_3}\right\} = Y^2$$

$$4\left\{\frac{tX}{4t^3-g_2t-g_3}\right\}^3 - \left\{\frac{tX}{4t^3-g_2t-g_3}\right\}\left[\frac{g_2}{(4t^3-g_2t-g_3)^2}\right] - \left\{\frac{g_3}{(4t^3-g_2t-g_3)^3}\right\}$$
$$= \left\{\frac{Y}{4t^3-g_2t-g_3}\right\}^2$$

Set $\mathbb{X} = \dfrac{tX}{4t^3-g_2t-g_3}$ $\qquad$ $\mathbb{Y} = \dfrac{Y}{4t^3-g_2t-g_3}$

$$4\Upsilon^3 - \left\{\frac{g_2}{(4t^3-g_2t-g_3)^2}\right\} \cdot \Upsilon - \left\{\frac{g_3}{(4t^3-g_2t-g_3)^3}\right\} = \Upsilon^2$$

Determine the modular invariant of C_2:

$$= 2^6 \cdot 3^3 \cdot \frac{\dfrac{g_2^3}{(4t^3-g_2t-g_3)^6}}{\dfrac{g_2^3}{(4t^3-g_2t-g_3)^6} - 27 \cdot \dfrac{g_3^2}{(4t^3-g_2t-g_3)^6}} = 2^6 \cdot 3^3 \cdot \frac{g_2^3}{g_2^3-27g_3^2}$$

= modular invariant of C_1.

Remark 3

It is important to emphasize that for particular $g_2, g_3 \in \mathbb{Q}$, in fact, for thirteen explicit pairs of g_2 and g_3, we get thirteen associated elliptic curves admitting complex multiplication in some imaginary quadratic field K, of class number one. In effect these thirteen elliptic curves will correspond to thirteen diophantine equations whose form is described by statement (1). So when we determine general solutions of the cubic curve (1) by the addition formulas, we are actually determining the solutions of the thirteen respective diophantine equations given by the particular $g_2, g_3 \in \mathbb{Q}$. Although we will describe the explicit method for deriving general solutions to the general form described by diophantine equation (1), it may be more productive to attack the problem directly - by determining rational solutions, through the addition theorems of one of the respective thirteen diophantine equations each having explicit g_2, g_3. This point will be attempted in particular for those diophantine equations corresponding to the

imaginary quadratic fields, $K = \mathbb{Q}(\sqrt{-2})$ and $K = \mathbb{Q}(\sqrt{-7})$. In general, the rational solution $(x(t),y(t))$ and its associated multiplier, λ satisfies statement (6) below.

2.2: Determining the associated complex multiplier λ to any given rational solution $(x(t),y(t))$.

Theorem 2. In the process of describing any given rational solution $(x(t),y(t))$ of diophantine equation (1), i.e.,

$$x(t) = \frac{p(\lambda u+\mu)}{p(u)} \qquad y(t) = \frac{p'(\lambda u+\mu)}{p'(u)} \qquad t = p(u)$$

$$\mu = 0,\ \omega_1,\ \omega_2,\ \omega_1 + \omega_2 = \omega_3$$

we find that the unique complex (or real) multiplier λ, associated with the given $(x(t),y(t))$ satisfies

$$\lambda y(t) = tx'(t) + x(t) = d(tx(t))/dt \tag{6}$$

Proof. The above remarks show that the rational solutions $(x(t),y(t))$ of

$$4t^3x(t)^3 - g_2tx(t) - g_3 = y(t)^2(4t^3-g_2t-g_3)$$
$$g_2,g_3 \in \mathbb{Q} \qquad\qquad g_2^3 - 27g_3^2 \neq 0$$

are constructed by use of the Weierstrass elliptic functions $(p(u),p'(u))$ parametrizing the curve $w^2 = 4t^3 - g_2t - g_3$ (7) whose respective lattice L_1 admits complex multiplication by λ. The abelian differential of the first kind corresponding to the Riemann surface generated by curve (7) is given by $dt/w = du$. We consider the lattice, L_2, obtained by multiplying each element, u of L_1 by the complex (real) multiplier λ and

then translating by μ. L_2 is associated with the Weierstrass equation

$$W^2 = 4T^3 - g_2T - g_3 \tag{8}$$

defined by $T = p(\lambda u+u)$ $W = p'(\lambda u+\mu)$ $\mu = 0, \omega_1, \omega_2, \omega_1 + \omega_2$

The abelian differential of the first kind corresponding to the Riemann surface generated by curve (8) is given by $dT/W = dU$. In particular, we have

$$\frac{dT}{W} = \frac{d(p(\lambda u+\mu))}{p'(\lambda u+\mu)} = \frac{\lambda p'(\lambda u+\mu)}{p'(\lambda u+\mu)} \quad du = \lambda du = \lambda \frac{dt}{w} . \tag{9}$$

Since, complex multiplication by λ produces the construction in which the ratio of the areas of the lattices, L_1 to L_2, $L_2 = \lambda L_1 \subseteq L_1$, is n = norm λ, this induces the endomorphism α from L_1 to L_2 in which n points of L_1 go to one point of L_2. We define mapping α from curve (7) to curve (8) by

$$T = tx(t) \qquad W = wy(t) \tag{9'}$$

in which n-values of t determined by tx(t) (and all associated with a respective w) give rise, under α to <u>one</u> value of T (associated with a respective W). According to statements (9) and (9') we select the associated λ to the rational solution (x(t),y(t)):

$$\frac{dT}{W} = \frac{tx'(t) + x(t)}{y(t)} \qquad \frac{dt}{w} = \lambda \frac{dt}{w}$$

i.e., $\lambda = \frac{tx'(t) + x(t)}{y(t)} \Rightarrow \lambda y(t) = tx'(t) + x(t) = d(tx(t))/dt$

<u>Example 1</u>. By the addition formulas of diophantine equation (1),

to be described shortly, we find that $\lambda = 2$, is associated with the rational solution

$$x(t) = \frac{t^4+(g_2/2)t^2+2g_3t+(g_2^2/16)}{4t(t^3-(g_2/4)t-(g_3/4))}$$

$$y(t) = \frac{t^6-(5g_2/4)t^4-5g_3t^3-(5g_2^2/16)t^2-(g_2g_3/4)t+(g_2^3-32g_3^2/64)}{8(t^3-(g_2/4)t-(g_3/4))^2} \qquad (10)$$

Not only does this choice of $(x(t),y(t))$ associated with $\lambda = 2$, satisfy equation (6), but that $\alpha:L_1 \to L_2$ defines a four to one mapping (norm $\lambda = 4$) in which <u>any</u> given value of T arises from four values of t, determined by checking the value of $tx(t) - T = 0$.

<u>Example 2</u>. Theorem 2 also enables us to determine the multiplier λ if we have already determined the rational solution $(x(t),y(t))$. For if $x(t) = y(t) = 1$, a solution of diophantine equation (1), we find, by statement (6), the associated λ is $\lambda = 1$.

<u>Corollary 2</u>. For general solutions $(x(t),y(t))$ of diophantine equation (1), the $\deg\{tx(t)\} = n$ where degree is taken to mean the higher (or equal) degree of the numerator or denominator of $tx(t)$.

2.3: Constructing rational solutions by the addition theorems

Since diophantine equation (1) is a cubic curve over $\mathbb{C}(t)$, there is a method which explicitly describes how to construct rational points on the curve from a known set S of rational points $P_1,P_2,\ldots,P_n$. By using the addition theorems of elliptic function theory, we can derive the secant and tangent

formulas for diophantine equation (1). We recall that solutions $(x(t),y(t))$ of diophantine equation (1) arise from solutions $(A(u),B(u))$ of equation (4) whereby $x(t) = A(u)/p(u)$; $y(t) = B(u)/p'(u)$, by condition (3'). In addition, not only does any $(x(t),y(t))$ correspond to some argument u, but by theorem 1 and lemma 1 each $(x(t),y(t))$ corresponds to some complex (or real) multiplier λ. Thus, the addition theorems of elliptic function theory are applied to diophantine equation (1) in the form:

$$\lambda_1 + \lambda_2 + \lambda_3 \equiv 0 \mod\{2\omega_1, 2\omega_2\}$$

$$\leftrightarrow \begin{vmatrix} 1 & 1 & 1 \\ x_1(t) & x_2(t) & x_3(t) \\ y_1(t) & y_2(t) & y_3(t) \end{vmatrix} = 0$$

whereby $\lambda_i \leftrightarrow (X_i(t),Y_i(t))$, $\mu = 0$.

In this context, the addition theorem presupposes that there is a relationship between the additive structure of the ring of integers of the imaginary quadratic field K which contains the multiplier λ_i, and the additive structure of rational solutions $(x_i(t),y_i(t))$ of the cubic curve (1).

The equation $Y^2 = 4X^3 - g_2X - g_3$ is parametrized by Weierstrass elliptic functions $(p(u),p'(u))$ where the series for $p(u)$ associated with the corresponding lattice $L = [2\omega_1,2\omega_2]$ is described as:

$$p(u) = \frac{1}{u^2} + \frac{g_2}{2^2\cdot 5}u^2 + \frac{g_3}{2^2\cdot 7}u^4 + \frac{g_2^2}{2^4\cdot 3\cdot 5^2}u^6 + \frac{3g_2g_3}{2^4\cdot 5\cdot 7\cdot 11}u^8 + \frac{2\cdot 3\cdot 5^3g_3^2+7^2g_2^3}{2^5\cdot 3\cdot 5^3\cdot 7^2\cdot 13}u^{10} + \ldots$$

subject to bounded u - away from the lattice points. In the secant formulas we will consider the equation

$$(X_1,Y_1) + (X_2,Y_2) = (X,Y)$$

whereby (X_1,Y_1) and (X_2,Y_2) are two different solutions over $\mathfrak{C}(t)$ of diophantine equation (1) which add in the sense of addition of points on a cubic curve to the sum, over $\mathfrak{C}(t)$, (X,Y). In the tangent formulas we allow for the case whereby

$$(X_1,Y_1) = (X_2,Y_2),$$

i.e.,

$$2(X_1,Y_1) = (X_0,Y_0)$$

The derivation of the tangent formulas uses dy/dx for the

$$\frac{\text{change in } y}{\text{change in } x}.$$

Secant

$$x(t) = \left\{\frac{t^3-(g_2/4)t-(g_3/4)}{t^3}\right\}\left[\frac{y_2-y_1}{x_2-x_1}\right]^2 - x_1 - x_2$$

$$y(t) = -\left\{\frac{t^3-(g_2/4)t-(g_3/4)}{t^3}\right\}\left[\frac{y_2-y_1}{x_2-x_1}\right]^3 + \frac{x_2y_2-x_1y_1+2(x_1y_2-x_2y_1)}{x_2-x_1} \qquad (11)$$

Tangent

$$\frac{dy}{dx} = \frac{t\{12t^2x(t)^2-g_2\}}{2\{4t^3-g_2t-g_3\}y(t)} \qquad \text{Set } tx(t) = X$$

$$x_0(t) = \frac{X^4+(g_2/2)X^2+2g_3X+(g_2^2/16)}{4t(X^3-(g_2/4)X-(g_3/4))}$$

$$y_0(t) = \frac{X^6-(5g_2/4)X^4-5g_3X^3-(5g_2^2/16)X^2-(g_2g_3/4)X+(g_2^3-32g_3^2)/64}{8(t^3-(g_2/4)t-(g_3/4))(X^3-(g_2/4)X-(g_3/4))y(t)}$$

(The solution exemplified in statement (10) is found by determining 2(1,1)).

There are precisely two cases under consideration:

Case 1: $d \equiv 2,3 \pmod 4$

Case 2: $d \equiv 1 \pmod 4$

We will illustrate each case by example.

Solutions arising from $\mu \neq 0$ will be described subsequently.

Case 1: $d \equiv 2,3 \pmod 4$ $\qquad d < 0 \quad \lambda \in C^*$

$$x(t) = \frac{p(\lambda u+\mu)}{p(u)} \qquad y(t) = \frac{p'(\lambda u+\mu)}{p'(u)}$$

$$(1,1) \quad \leftrightarrow \quad \lambda = 1, \mu = 0$$

and

$$\left(\frac{p(\sqrt{d}u)}{p(u)}, \frac{p'(\sqrt{d}u)}{p'(u)}\right) \quad \leftrightarrow \quad \lambda = \sqrt{d}, \mu = 0$$

All solutions arise from complex (or real) multiplications by the addition formulas as follows:

$$a(1,1) + b\left(\frac{p(\sqrt{d}u)}{p(u)}, \frac{p'(\sqrt{d}u)}{p'(u)}\right) \leftrightarrow \lambda = a + b\sqrt{d} \qquad (11')$$

$$a,b \in \mathbb{Z}$$

$$\text{norm } \lambda = a^2 - b^2 d$$

The lattice L_1, associated with the equation $y^2 = 4x^3 - g_2x - g_3$ is of the form $[\xi, \xi\sqrt{d}]$ where ξ is the real period and $\xi\sqrt{d}$ is the imaginary period. Under complex multiplication by λ, lattice L_1 will be shifted to lattice $L_2 = [\xi, \xi\lambda]$ where

$$[\xi, \xi\lambda] \subseteq [\xi, \xi\sqrt{d}]$$

Example 3. $K = \mathbb{Q}(\sqrt{-2}) \qquad f = 1$

According to Hadano (see [5], pg. 92) the corresponding

Weierstrass model is

$$B^2 = A^3 + 4A^2 + 2A$$

Let $B \to B$, $A \to A - \frac{4}{3}$. This gives the form:

$$B^2 = A^3 + (-10/3)A + (56/27)$$

$$= (A-(4/3))(A-(-2+3\sqrt{2})/3)(A-(-2-3\sqrt{2})/3)$$

so that

$$g_2 = \frac{40}{3} \qquad g_3 = -\frac{224}{27} \qquad J_L = 20^3$$

Upon setting $A = A(u) = x(t)p(u)$

$$B = B(u) = y(t)p'(u)$$

$$p(u) = -2t/3$$

and using the fact

$$p'(u)^2 = p^3(u) - (10/3)p(u) + (56/27)$$

We get the form described by diophantine equation (1):

$$2t^3x(t)^3 - 15tx(t) - 14 = y^2(t)(2t^3-15t-14)$$

$$= y^2(t)(2t^2-4t-7)(t+2)$$

The above elliptic curve admits complex multiplication by $\lambda = a + b\sqrt{-2}$; $a,b \in \mathbb{Z}$ norm $\lambda = a^2 + 2b^2$. Its associated lattice L is of the form $[\xi, \xi\sqrt{-2}]$ where

$$\xi = 2\int_{4/3}^{\infty} \frac{dx}{\sqrt{4x^3-(40/3)x+(224/27)}}$$

Under complex multiplication by $\lambda \in [1, \sqrt{-2}]$, the ring of integers of $\mathbb{Q}(\sqrt{-2})$ we have $[\xi, \xi\lambda] \subseteq [\xi, \xi\sqrt{-2}]$.

In addition, the above elliptic curve is parametrized by Weierstrass functions $(p(u), p'(u))$ whereby

$$p(u) = \frac{1}{u^2} + \frac{2}{3}u^2 - \frac{8}{27}u^4 + \frac{4}{27}u^6 - \frac{16}{297}u^8 + \frac{208}{9477}u^{10} + \ldots$$

The addition formulas ($\mu = 0$) for the given diophantine equation are described as:

Secant

$$x(t) = \left\{\frac{(t^2-2t-(7/2))(t+2)}{t^3}\right\}\left[\frac{y_2-y_1}{x_2-x_1}\right]^2 - x_1 - x_2$$

$$y(t) = -\left\{\frac{(t^2-2t-(7/2))(t+2)}{t^3}\right\}\left[\frac{y_2-y_1}{x_2-x_1}\right]^3 + \frac{x_2y_2-x_1y_1+2(x_1y_2-x_2y_1)}{x_2-x_1}$$

Tangent

$$\left(\frac{dy}{dx}\right)_{(x_1,y_1)} = \frac{t(6t^2x_1^2-15)}{4(t^2-2t-(7/2))(t+2)y_1} \qquad tX_1(t) = X$$

$$x_0(t) = \frac{X^4+15X^2+56X+(225/4)}{4t(X^2-2X-(7/2))(X+2)}$$

$$y_0(t) = \frac{X^6-(75/2)X^4-140X^3-(1125/4)X^2-210X+(239/8)}{8(t^2-2t-(7/2))(t+2)(X^2-2X-(7/2))(X+2)y_1}$$

All solutions arise from complex (or real) multiplications by the addition formulas as follows:

$$a(1,1) + b\left(\frac{p(\sqrt{-2}u)}{p(u)}, \frac{p'(\sqrt{-2}u)}{p'(u)}\right) \leftrightarrow \lambda = a + b\sqrt{-2}, \quad \mu = 0$$

in which

the rational solution (1,1) $\leftrightarrow \lambda = 1, \quad \mu = 0$

and

the rational solution $\left(\frac{p(\sqrt{-2}u)}{p(u)}, \frac{p'(\sqrt{-2}u)}{p'(u)}\right) \leftrightarrow \lambda = \sqrt{-2}, \ \mu = 0$

We note $\frac{p(\sqrt{-2}u)}{p(u)}$ and $\frac{p'(\sqrt{-2}u)}{p'(u)}$ are by lemma 1, rational functions in t, and are determined as follows:

Upon considering the period parallelogram generated by $[1,\sqrt{-2}]$ we use a cancellation of zeros and poles argument which yields

the following form:

$$2p(\sqrt{-2}u) + p(u) = \frac{A}{p(u)-p(1/\sqrt{-2})}$$

Basically, by using the series for $p(u)$ and complex multiplication by $\sqrt{-2}$, the left side has a zero of order 2 at $u = 0$ and a pole of order 2 at $u = \sqrt{-2}/2$; while the expression $p(u) - p(1/\sqrt{-2})$ has a pole of order 2 at $u = 0$ and a zero of order 2 at $u = \sqrt{-2}/2$. This implies by Liouville's theorem,

$$\{2p(\sqrt{-2}u) + p(u)\}\{p(u) - p(1/\sqrt{-2})\}$$

has no residue classes of poles and is bounded in the fundamental period parallelogram and/or the whole plane; and is thereby a constant, A.

Then

$$\frac{p(\sqrt{-2}u)}{p(u)} = -\frac{1}{2} + \frac{A}{p(u)(p(u)-B)} \qquad B = p(1/\sqrt{-2})$$

$$x(p(u)) = \frac{p(\sqrt{-2}u)}{p(u)} = -\frac{1}{2} + \frac{-1}{p(u)(p(u)-(4/3))}$$

whereby $A = -1$, $B = 4/3$ are determined by applying the series for $p(u)$ to both sides of the preceding equation. Setting $p(u) = -2t/3$ in the preceding expression

$$x(t) = -\frac{1}{2} + \frac{-1}{(-2t/3)((-2t/3)-(4/3))} = \frac{-2t^2-4t-9}{4t(t+2)}$$

$$= \frac{t^2+2t+(9/2)}{-2t(t+2)}$$

From the derivative of $p(\sqrt{-2}u)$ determined from the above expression for $p(\sqrt{-2}u)$ we find

$$y(p(u)) = \frac{p'(\sqrt{-2}u)}{p'(u)} = -\frac{1}{2\sqrt{-2}} + \frac{1/\sqrt{-2}}{(p(u)-(4/3))^2}$$

Setting $p(u) = -2t/3$

$$y(t) = \frac{-2t^2-8t+1}{4\sqrt{-2}(t+2)^2} = \frac{t^2+4t-(1/2)}{-2\sqrt{-2}(t+2)^2}$$

Therefore, all solutions arise from complex (or real) multiplications by the addition formulas as follows:

$$a(1,1) + b\left(\frac{t^2+2t+(9/2)}{-2t(t+2)}, \frac{t^2+4t-(1/2)}{-2\sqrt{-2}(t+2)^2}\right) \leftrightarrow \lambda = a+b\sqrt{-2},\ \mu = 0$$

Case 2: $d \equiv 1 \pmod 4$ $\quad d < 0 \quad \lambda \in C^*$

$$x(t) = \frac{p(\lambda u+\mu)}{p(u)} \qquad y(t) = \frac{p'(\lambda u+\mu)}{p'(u)}$$

$$(1,1) \leftrightarrow \lambda = 1,\ \mu = 0$$

and

$$\left(\frac{p(\frac{1+\sqrt{d}}{2}u)}{p(u)}, \frac{p'(\frac{1+\sqrt{d}}{2}u)}{p'(u)}\right) \leftrightarrow \lambda = \frac{1+\sqrt{d}}{2},\ \mu = 0$$

All solutions arise from complex (or real) multiplications by the addition formulas as follows:

$$a(1,1) + b\left(\frac{p(\frac{1+\sqrt{d}}{2}u)}{p(u)}, \frac{p'(\frac{1+\sqrt{d}}{2}u)}{p'(u)}\right) \leftrightarrow \lambda = (a+(b/2))+(b/2)\sqrt{d}$$

$$a,b \in \mathbb{Z}$$

$$\text{norm } \lambda = a^2+ab+(\frac{1-d}{4})b^2$$

The lattice L_1, associated with the equation $Y^2 = 4X^3-g_2X-g_3$ is of the form $[\xi, \xi(\frac{1+\sqrt{d}}{2})]$ where ξ is the real period and $\xi(\frac{1+\sqrt{d}}{2})$ is the imaginary period. Complex multiplication by λ will again introduce the appropriate shift in L_1.

Example 4. $K = \mathbb{Q}(\sqrt{-7})$ $\quad f = 1$

According to Hadano (see [5], pg. 93), the corresponding Weierstrass model is

$$B^2 = A^3 + 21A^2 + 112A$$

Let $B \to B$, $A \to A-7$. This gives the form:

$$B^2 = A^3 - 35A - 98$$
$$= (A-7)(A-(-7+\sqrt{-7})/2)(A-(-7-\sqrt{-7})/2)$$

so that

$$g_2 = 140 = 2^2 \cdot 5 \cdot 7 \qquad g_3 = 392 = 2^3 \cdot 7^2 \qquad J_L = -15^3$$

Upon setting $A = A(u) = x(t)p(u)$

$$B = B(u) = y(t)p'(u)$$

$$p(u) = t$$

and using the fact

$$p'(u)^2 = p^3(u) - 35p(u) - 98$$

we get the form described by diophantine equation (1):

$$t^3x(t)^3 - 35tx(t) - 98 = y^2(t)(t^3-35t-98)$$
$$= y^2(t)(t^2+7t+14)(t-7)$$

The above elliptic curve admits complex multiplication by

$\lambda = (a+(b/2)) + (b/2)\sqrt{-7}$; $a,b \in \mathbb{Z}$ norm $\lambda = a^2 + ab + 2b^2$

Its associated lattice L is of the form $[\xi, \xi(\frac{1+\sqrt{-7}}{2})]$ where

$$\xi = 2\int_7^\infty \frac{dx}{\sqrt{4x^3-140x-392}}$$

Under complex multiplication by $\lambda \in [1, \frac{1+\sqrt{-7}}{2}]$, the ring of integers of $\mathbb{Q}(\sqrt{-7})$ we have $[\xi, \xi\lambda] \subseteq [\xi, \xi(\frac{1+\sqrt{-7}}{2})]$.

In addition, the above elliptic curve is parameterized by Weierstrass functions $(p(u), p'(u))$ whereby

$$p(u) = \frac{1}{u^2} + 7u^2 + 14u^4 + \frac{49}{3}u^6 + \frac{294}{11}u^8 + \frac{98}{3}u^{10} + \ldots$$

The addition formulas ($u = 0$) for the given diophantine equation

are determined by setting $g_2 = 140$, $g_3 = 392$ in statement (11):

Secant

$$x(t) = \left\{\frac{(t^2+7t+14)(t-7)}{t^3}\right\}\left[\frac{y_2-y_1}{x_2-x_1}\right]^2 - x_1 - x_2$$

$$y(t) = -\left\{\frac{(t^2+7t+14)(t-7)}{t^3}\right\}\left[\frac{y_2-y_1}{x_2-x_1}\right]^3 + \frac{x_2y_2-x_1y_1+2(x_1y_2-x_2y_1)}{x_2-x_1}$$

Tangent

$$\left(\frac{dy}{dx}\right)_{(x_1,y_1)} = \frac{t(3t^2x_1^2-35)}{2(t^2+7t+14)(t-7)y_1} \qquad tx_1(t) = X$$

$$x_0(t) = \frac{X^4+70X^2+784X+1225}{4t(X^2+7X+14)(X-7)}$$

$$y_0(t) = \frac{X^6-175X^4-1960X^3-6125X^2-13720X-33957}{8(t^2+7t+14)(t-7)(X^2+7X+14)(X-7)y_1}$$

All solutions arise from complex (or real) multiplications by the addition formulas as follows:

$$a(1,1)+b\left(\frac{p(\frac{1+\sqrt{-7}}{2}u)}{p(u)}, \frac{p'(\frac{1+\sqrt{-7}}{2}u)}{p'(u)}\right) \leftrightarrow \lambda = (a+(b/2))+(b/2)\sqrt{-7},\ \mu = 0$$

in which the rational solution

$$(1,1) \qquad \leftrightarrow \lambda = 1,\ \mu = 0$$

and the rational solution

$$\left(\frac{p(\frac{1+\sqrt{-7}}{2}u)}{p(u)}, \frac{p'(\frac{1+\sqrt{-7}}{2}u)}{p'(u)}\right) \leftrightarrow \lambda = \frac{1+\sqrt{-7}}{2},\ \mu = 0$$

$\frac{p(\frac{1+\sqrt{-7}}{2}u)}{p(u)}$ and $\frac{p'(\frac{1+\sqrt{-7}}{2}u)}{p'(u)}$ are rational functions in t and are determined, as in example 3, $K = \mathbb{Q}(\sqrt{-2})$, by a cancellation of zeros and poles argument which yields the following form:

$$\left(\frac{-3+\sqrt{-7}}{2}\right) p\left(\frac{1+\sqrt{-7}}{2}u\right) - p(u) = \frac{A}{p(u) - p\left(\frac{3+\sqrt{-7}}{4}\right)}$$

By using the series for $p(u)$ and complex multiplication by $\frac{1+\sqrt{-7}}{2}$, the left side has a zero of order 2 at $u = 0$ and a pole of order 2 at $u = \frac{3+\sqrt{-7}}{4}$.

The expression $p(u) - p\left(\frac{3+\sqrt{-7}}{4}\right)$ has a pole of order 2 at $u = 0$ and a zero of order 2 at $u = \frac{3+\sqrt{-7}}{4}$. By Liouville's theorem we get the described form. Then,

$$\frac{p\left(\frac{1+\sqrt{-7}}{2}u\right)}{p(u)} = \frac{1}{\left(\frac{-3+\sqrt{-7}}{2}\right)} + \frac{A}{p(u)\,(p(u)-B)} \qquad B = p\left(\frac{3+\sqrt{-7}}{4}\right)$$

$$x(p(u)) = \frac{p\left(\frac{1+\sqrt{-7}}{2}u\right)}{p(u)} = \frac{1}{\left(\frac{-3+\sqrt{-7}}{2}\right)} + \frac{(7/8)(-9+5\sqrt{-7})}{p(u)\left(p(u)-\left(\frac{-7+\sqrt{-7}}{2}\right)\right)}$$

whereby $A = \frac{7}{8}(-9+5\sqrt{-7})$, $B = \frac{-7+\sqrt{-7}}{2}$ are determined by applying the series for $p(u)$ to both sides of the preceding equation. Setting $p(u) = t$ in the preceding expression:

$$x(t) = \frac{1}{\left(\frac{-3+\sqrt{-7}}{2}\right)} + \frac{(7/8)(-9+5\sqrt{-7})}{t\left(t-\left(\frac{-7+\sqrt{-7}}{2}\right)\right)}$$

$$= \frac{t(8t+28-4\sqrt{-7}) + 7(-9+5\sqrt{-7})\left(\frac{-3+\sqrt{-7}}{2}\right)}{\left(\frac{-3+\sqrt{-7}}{2}\right) t(8t+28-4\sqrt{-7})}$$

$$= \frac{8t^2+28t-4t\sqrt{-7}+(-28-84\sqrt{-7})}{\left(\frac{-3+\sqrt{-7}}{2}\right) 8t\left(t+(7/2)-(1/2)\sqrt{-7}\right)}$$

$$= \frac{t^2+\left((7/2)-(1/2)\sqrt{-7}\right)\ t+\left((-7/2)-(21/2)\sqrt{-7}\right)}{\left(\frac{-3+\sqrt{-7}}{2}\right) t\left(t+(7/2)-(1/2)\sqrt{-7}\right)}$$

From the derivative of $p(\frac{1+\sqrt{-7}}{2}u)$ determined from the above expression for $p(\frac{1+\sqrt{-7}}{2}u)$ we find

$$y(p(u)) = \frac{p'(\frac{1+\sqrt{-7}}{2}u)}{p'(u)} = \frac{1}{(\frac{-5-\sqrt{-7}}{2})} + \frac{(-7/16)(13+7\sqrt{-7})}{(p(u)-(\frac{-7+\sqrt{-7}}{2}))^2}$$

Setting $p(u) = t$

$$y(t) = \frac{1}{(\frac{-5-\sqrt{-7}}{2})} + \frac{(-7/16)(13+7\sqrt{-7})}{(t+(7/2)-(1/2)\sqrt{-7})^2}$$

$$= \frac{t^2+(7-\sqrt{-7})t+(14+7\sqrt{-7})}{(\frac{-5-\sqrt{-7}}{2})(t+(7/2)-(1/2)\sqrt{-7})^2}$$

Therefore all solutions arise from complex (or real) multiplications by the addition formulas as follows:

$a(1,1) +$

$$b\left[\frac{t^2+((7/2-(1/2)\sqrt{-7})t+(-(7/2)-(21/2)\sqrt{-7})}{(\frac{-3+\sqrt{-7}}{2})t(t+(7/2)-(1/2)\sqrt{-7})^2}, \frac{t^2+(7-\sqrt{-7})t+(14+7\sqrt{-7})}{(\frac{-5-\sqrt{-7}}{2})(t+(7/2)-(1/2)\sqrt{-7})^2}\right.$$

$$\leftrightarrow \quad \lambda = (a+(b/2)) + (b/2)\sqrt{-7} \quad , \mu = 0$$

The above section deals with the construction of rational solutions $(x(t),y(t))$, which correspond to a non-zero complex (or real) multiplier λ and a <u>zero</u> μ. For general d, how does one construct rational solutions of diophantine equation (1), which correspond to a non-zero λ and a <u>non-zero</u> μ? Recall that the equation $Y^2 = 4X^3 - g_2X - g_3$, parametrized by $X = p(u)$, $Y = p'(u)$, factors, on the right side as follows:

$$Y^2 = (X-e_1)(X-e_2)(X-e_3) \quad e_i \in \mathbb{C}$$

By the theory this means $X = e_i$ when $u = \omega_i$, $i = 1,2,3$. We determine $p(u+\omega_i)$, and therefore $p'(u+\omega_i)$ by the following formula from elliptic function theory (see [4], pg. 20).

$$p(u+\omega_i) = \frac{e_i p(u)+(2e_i^2-(1/4)g_2)}{p(u)-e_i}\ , \quad g_2 \in \Phi \tag{12}$$

In particular, $p(\lambda u+\omega_i)$ is determined by substituting λu for u on the right side of statement (12). This implies

$$\begin{aligned} x(t) &= \frac{p(\lambda u+\omega_i)}{p(u)} = \frac{e_i p(\lambda u)+(2e_i^2-(g_2/4))}{p(u)(p(\lambda u)-e_i)}\ , \ t = p(u) \\ y(t) &= \frac{p'(\lambda u+\omega_i)}{p'(u)} = \frac{-3e_i^2+(g_2/4)}{(p(\lambda u)-e_i)^2}\ , \ t = p(u). \end{aligned} \tag{12'}$$

We determine the expression for $p(\lambda u) = p(u)x(p(u))$, $t = p(u)$, from the addition formulas described by statement (11), for the case $\mu = 0$.

Example 5. Suppose d is unspecified, $\lambda = 1$, $\mu = \omega_i$, then

$$x(t) = \frac{e_i p(u)+(2e_i^2-(g_2/4))}{p(u)(p(u)-e_i)} = \frac{e_i t+(2e_i^2-(g_2/4))}{t(t-e_i)}\ , \ p(u) = t$$

$$y(t) = \frac{-3e_i^2+(g_2/4)}{(p(u)-e_i)^2} = \frac{-3e_i^2+(g_2/4)}{(t-e_i)^2}$$

and e_i, $i = 1,2,3$ are the roots of the equation

$$4x^3 - g_2x - g_3 = 0.$$

Example 6. Suppose d is unspecified, $\lambda = 2$, $\mu = \omega_i$, then

$$x(p(u)) = \frac{e_i p(2u)+(2e_i^2-(g_2/4))}{p(u)(p(2u)-e_i)}\ .$$

By statement (10)

$$\frac{p(2u)}{p(u)} = \frac{p(u)^4+(g_2/2)p(u)^2+2g_3p(u)+(g_2^2/16)}{4p(u)(p(u)^3-(g_2/4)p(u)-(g_3/4))}$$

We substitute

$$p(2u) = \frac{p(u)^4+(g_2/2)p(u)^2+2g_3p(u)+(g_2^2/16)}{4(p(u)^3-(g_2/4)p(u)-(g_3/4))}$$

into our expression for $x(p(u))$ and then set $p(u) = t$ to get

$$x(t) = \frac{\{e_it^4+(8e_i^2-g_2)t^3+(g_2/2)e_it^2+(2g_3e_i-2g_2e_i^2+(g_2^2/4))t + ((g_2^2/16)e_i-2e_i^2g_3+(g_2g_3/4))\}}{t(t^4-4e_it^3+(g_2/2)t^2+(g_2e_i+2g_3)t+((g_2^2/16)+g_3e_i))}$$

$$y(p(u)) = \frac{-3e_i^2+(g_2/4)}{(p(2u)-e_i)^2} .$$

After substituting for $p(2u)$ and setting $p(u) = t$ in the resulting expression we get:

$$y(t) = \frac{((-48e_i^2+4g_2)t^6+(24g_2e_i^2-2g_2^2)t^4+(24g_3e_i^2-2g_2g_3)t^3 + (-3e_i^2g_2^2+(g_2^3/4))t^2+(-6e_i^2g_2g_3+(g_2^2g_3/2))t +((g_2g_3^2)/4)-3e_i^2g_3^2)}{(t^4-4e_it^3+(g_2/2)t^2+(g_2e_i+2g_3)t+((g_2^2/16)+g_3e_i))^2}$$

Let us conclude our discussion with the construction of rational solutions, corresponding to a non-zero λ and a non-zero μ, by applying the results of the above example 5, d unspecified, $\lambda = 1$, $\mu = \omega_i$ to the two cases; case 1, $K = \mathbb{Q}(\sqrt{-2})$ and case 2, $K = \mathbb{Q}(\sqrt{-7})$.

<u>Case 1</u>. $K = \mathbb{Q}(\sqrt{-2})$ $g_2 = 40/3$ $g_3 = -224/27$ $p(u) = -2t/3$

$$Y^2 = X^3-(10/3)X+(56/27)$$

$$= (X-(4/3))(X-(-2+3\sqrt{2})/3)(X-(-2-3\sqrt{2})/3).$$

Let a) $\mu = \omega_1$ correspond to $X = 4/3 = e_1$

b) $\mu = \omega_2$ correspond to $X = (-2+3\sqrt{2})/3 = e_2$

c) $\mu = \omega_3$ correspond to $X = (-2-3\sqrt{-2})/3 = e_3$

The corresponding formulas to statement (12') are

$$x(p(u)) = \frac{e_i p(\lambda u)+(2e_i^2-(10/3))}{p(u)(p(\lambda u)-e_i)}$$

$$y(p(u)) = \frac{-3e_i^2+(10/3)}{(p(\lambda u)-e_i)^2}$$

For $\lambda = 1$, $\mu = \omega_i$, $p(\lambda u) = p(u)$, e_i unspecified

$$x(t) = \frac{e_i(-2t/3)+(2e_i^2-(10/3))}{(-2t/3)((-2t/3)-e_i)} = \frac{-6e_i(t-3e_i+(5/e_i))}{4t(t+(3e_i/2))}$$

$$y(t) = \frac{3(-9e_i^2+10)}{(-2t-3e_i)^2} = \frac{3(-9e_i^2+10)}{4(t+(3e_i/2))^2}$$

a) $\lambda = 1$, $\mu = \omega_1$, $e_1 = 4/3$

$$x(t) = \frac{-2(t-(1/4))}{t(t+2)} \qquad y(t) = \frac{-9}{2(t+2)^2}$$

b) $\lambda = 1$, $\mu = \omega_2$, $e_2 = (-2+3\sqrt{2})/3$

$$x(t) = \frac{(-2+3\sqrt{2})\{t+(1/14)(58+3\sqrt{2})\}}{-2t(t+(-2+3\sqrt{2})/2)}$$

$$y(t) = \frac{-9(1-\sqrt{2})}{(t+(-2+3\sqrt{2})/2)^2}$$

c) $\lambda = 1$, $\mu = \omega_3$, $e_3 = (-2-3\sqrt{2})/3$

$$x(t) = \frac{(-2-3\sqrt{2})\{t+(1/14)(58-3\sqrt{2})\}}{-2t(t+(-2-3\sqrt{2})/2)}$$

$$y(t) = \frac{-9(1+\sqrt{2})}{(t+(-2-3\sqrt{2})/2)^2}$$

Case 2. $K = \mathbb{Q}(\sqrt{-7})$ $g_2 = 140$ $g_3 = 392$ $p(u) = t$

$$Y^2 = X^3 - 35X - 98$$

$$= (X-7)(X-(-7+\sqrt{-7})/2)(X-(-7-\sqrt{-7})/2)$$

Let a) $\mu = \omega_1$ correspond to $X = 7 = e_1$

b) $\mu = \omega_2$ correspond to $X = (-7+\sqrt{-7})/2 = e_2$

c) $\mu = \omega_3$ correspond to $X = (-7-\sqrt{-7})/2 = e_3$

The corresponding formulas to statement (12') are

$$x(p(u)) = \frac{e_i p(\lambda u)+(2e_i^2-35)}{p(u)(p(\lambda u)-e_i)}$$

$$y(p(u)) = \frac{-3e_i^2+35}{(p(\lambda u)-e_i)^2}$$

For $\lambda = 1$, $\mu = \omega_i$, $p(\lambda u) = p(u)$, e_i unspecified

$$x(t) = \frac{e_i t+(2e_i^2-35)}{t(t-e_i)}$$

$$y(t) = \frac{-3e_i^2+35}{(t-e_i)^2}$$

a) $\lambda = 1$, $\mu = \omega_1$, $e_1 = 7$

$$x(t) = \frac{7(t+9)}{t(t-7)} \qquad y(t) = \frac{-112}{(t-7)^2}$$

b) $\lambda = 1$, $\mu = \omega_2$, $e_2 = (-7+\sqrt{-7})/2$

$$x(t) = \frac{((-7+\sqrt{-7})/2)t+(-14-7\sqrt{-7})}{t(t+(7-\sqrt{-7})/2)}$$

$$y(t) = \frac{(7/2)(1+3\sqrt{-7})}{(t+(7-\sqrt{-7})/2)^2}$$

c) $\lambda = 1$, $\mu = \omega_3$, $e_3 = (-7-\sqrt{-7})/2$

$$x(t) = \frac{((-7-\sqrt{-7})/2)t+(-14+7\sqrt{-7})}{t(t+(7+\sqrt{-7})/2)}$$

$$y(t) = \frac{(7/2)(1-3\sqrt{-7})}{(t+(7+\sqrt{-7})/2)^2}$$

Remark 4. There are no rational solutions associated with the case $\lambda = 0$, $\mu = 0$; for in this situation $p(u)$ and $p'(u)$ are both undefined. This leaves us with the final case: construct the rational solutions $(x(t),y(t))$ which correspond to a zero multiplier λ and a non-zero μ.

2.4: Applications to the thirteen imaginary quadratic rings having class number one.

When $\lambda = 0$, $\mu = \omega_1, \omega_2, \omega_3$, the corresponding rational solutions to diophantine equation (1) take the form

$$x(t) = \frac{p(\omega_i)}{p(u)} = \frac{e_i}{t}, \quad i = 1,2,3 \qquad t = p(u)$$

$$y(t) = \frac{p'(\omega_i)}{p'(u)} = \frac{0}{\sqrt{4t^3-g_2t-g_3}} = 0$$

since

$$Y^2 = 4X^3 - g_2X - g_3$$
$$= (X-e_1)(X-e_2)(X-e_3)$$

and

$$X = e_i = p(\omega_i) \text{ when } Y = p'(\omega_i) = 0.$$

The ω_i are the non-zero torsion points of order 2 in the lattice L associated with the elliptic cure $Y^2 = 4X^3 - g_2X - g_3$. In particular, this means the following for general d:

Case 1: $d \equiv 2,3 \pmod 4$ $\quad d < 0$ $\quad d$ square free

$$L = [\xi, \xi\sqrt{d}]$$

$$p(\xi/2) = e_1, \quad p((\xi\sqrt{d})/2) = e_2, \quad p((\xi+\xi\sqrt{d})/2) = e_3.$$

So $(\frac{e_1}{t}, 0)$ corresponds to $\lambda = 0, \mu = \frac{\xi}{2}$

$(\frac{e_2}{t}, 0)$ corresponds to $\lambda = 0, \mu = \frac{\xi\sqrt{d}}{2}$

$(\frac{e_3}{t}, 0)$ corresponds to $\lambda = 0, \mu = \frac{\xi + \xi\sqrt{d}}{2}$

Case 2: $d \equiv 1 \pmod 4$ $\quad d < 0$ $\quad d$ square free

$$L = [\xi, \xi(\frac{1 + \sqrt{d}}{2})]$$

$$p(\frac{\xi}{2}) = e_1, \quad p(\frac{\xi(1+\sqrt{d})}{4}) = e_2, \quad p(\frac{\xi(3+\sqrt{d})}{4}) = e_3$$

So $(\frac{e_1}{t}, 0)$ corresponds to $\lambda = 0, \mu = \frac{\xi}{2}$

$(\frac{e_2}{t}, 0)$ corresponds to $\lambda = 0, \mu = \frac{\xi(1+\sqrt{d})}{4}$

$(\frac{e_3}{t}, 0)$ corresponds to $\lambda = 0, \mu = \frac{\xi(3+\sqrt{d})}{4}$

According to the addition formulas described by statement (11), the rational solutions $((e_i/t), 0)$, $i = 1,2,3$ are torsion points of order 2, of diophantine equation (1). At most, these points of order 2 form a subgroup of order four, over $\mathbb{Q}(t)$, namely

$$\{(\frac{e_1}{t}, 0), (\frac{e_2}{t}, 0), (\frac{e_3}{t}, 0), (\infty,\infty)\} \tilde{=} C_2 \times C_2.$$

Let us apply these results to the thirteen special cases. The following is a list of the thirteen elliptic curves $Y^2 = f(X)$ and their associated diophantine equations as developed by this paper. We will display the factors of f(x), when f(x) has one rational root. By applying the rational root theorem to each curve, we have found that it is never

the case that f(x) has two or three rational roots. Each diophantine equation was determined by substituting the appropriate pair g_2, g_3 into statement (1).

1. $d = -1$, $f = 1$.

   Equation $y^2=f(x)$; $Y^2=X^3+X = X(X-i)(X+i)$

   $g_2 = -4$, $g_3 = 0$

   Diophantine Equation: $4t^3x(t)^3+4tx(t) = y(t)^2(4t^2+4t)$

2. $d = -2$, $f = 1$.

   Equation $y^2=X^3-(^{10}/_3)X + (^{56}/_{27})$

   $= (X-\ ^4/_3)(X-(-\ ^2/_3\ +\sqrt{2}))(X-(\ -^2/_3\ -\sqrt{2}))$

   $g_2 = (^{40}/_3)$, $g_3 = (-^{224}/_{27})$

   Diophantine Equation: $4t^3x(t)^3-(^{40}/_3)tx(t) + (^{224}/_{27})$

   $= y(t)^2(4t^3-(^{40}/_3)t + (^{224}/_{27}))$

3. $d = -3$, $f = 1$.

   Equation $y^2 = X^3 + 1 = (X+1)(X-(\frac{1+\sqrt{3}}{2}))(X-(\frac{1-\sqrt{3}}{2}))$

   $g_2 = 0$, $g_3 = -4$

   Diophantine Equation: $4t^3x(t)^3+4 = y(t)^2(4t^3+4)$

4. $d = -7$, $f = 1$.

   Equation $y^2 = X^3-35X-98 = (X-7)(X-(\frac{-7+\sqrt{-7}}{2}))(X-(\frac{-7-\sqrt{-7}}{2}))$

   $g_2 = 140$, $g_3 = 392$

   Diophantine Equation: $4t^3x(t)^3-140tx(t)-392$

   $= y(t)^2(4t^3-140t-392)$

5. $d = -1$, $f = 2$.

   Equation $y^2=X^3-11X+14=(X-2)(X-(-1+2\sqrt{2}))(X-(-1-2\sqrt{2}))$

   $g_2 = 44$, $g_3 = -56$

   Diophantine Equation: $4t^3x(t)^3-44tx(t)+56=y(t)^2(4t^3-44t+56)$

6. $d = -3$, $f = 2$.

Equation $y^2 = X^3 - 15X + 22 = (X-2)(X-(-1+2\sqrt{3}))(X-(-1-2\sqrt{3}))$

$g_2 = 60$, $g_3 = -88$

Diophantine Equation: $4t^3x(t)^3 - 60tx(t) + 88 = y(t)^2(4t^3 - 60t + 88)$

7. $d = -7$, $f = 2$.

Equation $y^2 = X^3 - 595X - 5586 = (X+14)(X-(7+8\sqrt{7}))(X-(7-8\sqrt{7}))$

$g_2 = 2380$, $g_3 = 22344$

Diophantine Equation: $4t^3x(t)^3 - 2380tx(t) - 22344$
$= y(t)^2(4t^3 - 2380t - 22344)$

8. $d = -11$, $f = 1$.

Equation $y^2 = X^3 - 264X - 1694$

$g_2 = 1056$, $g_3 = 6776$

Diophantine Equation: $4t^3x(t)^3 - 1056tx(t) - 6776$
$= y(t)^2(4t^3 - 1056t - 6776)$

9. $d = -19$, $f = 1$.

Equation $y^2 = X^3 - 152X + 722$

$g_2 = 608$, $g_3 = -2888$

Diophantine Equation: $4t^3x(t)^3 - 608tx(t) + 2888$
$= y(t)^2(4t^3 - 608t + 2888)$

10. $d = -43$, $f = 1$.

Equation $y^2 = X^3 - 3440X + 77658$

$g_2 = 13760$, $g_3 = -310632$

Diophantine Equation: $4t^3x(t)^3 - 13760tx(t) + 310632$
$= y(t)^2(4t^3 - 4 \cdot 3440t + 310632)$

11. $d = -67$, $f = 1$.

Equation $y^2 = X^3 - 29480X + 1948226$

$g_2 = 4 \cdot 29480$, $g_3 = -4 \cdot 1948226$

Diophantine Equation: $4t^3x(t)^3 - 4 \cdot 29480tx(t) + 4 \cdot 1948226$
$= y(t)^2(4t^3 - 4 \cdot 29480t + 4 \cdot 1948226)$

12. $d = -163$, $f = 1$

Equation $y^2 = X^3 - 2^4 \cdot 5 \cdot 23 \cdot 29 \cdot 163X + 2 \cdot 7 \cdot 11 \cdot 19 \cdot 127 \cdot 163^2$

$g_2 = 2^6 \cdot 5 \cdot 23 \cdot 29 \cdot 163$, $g_3 = -2^3 \cdot 7 \cdot 11 \cdot 19 \cdot 127 \cdot 163^2$

Diophantine Equation: $4t^3x(t)^3 - 2^6 \cdot 5 \cdot 23 \cdot 29 \cdot 163tx(t)$
$+ 2^3 \cdot 7 \cdot 11 \cdot 19 \cdot 127 \cdot 163^2$
$= y(t)^2(4t^3 - 2^6 \cdot 5 \cdot 23 \cdot 29 \cdot 163t + 2^3 \cdot 7 \cdot 11 \cdot 19 \cdot 127 \cdot 163^2)$

13. $d = -3$, $f = 3$

Equation $y^2 = X^3 - 120X + 506$

$g_2 = 480$, $g_3 = -2024$

Diophantine Equation: $4t^3x(t)^3 - 480tx(t) + 2024$
$= y(t)^2(4t^3 - 480t + 2024)$

By observing this table, we arrive at the following results:

Theorem 3. 1) If $4t^3 - g_2t - g_3 = 0$ has one rational root e_1, then $Y^2 = 4X^3 - g_2X - g_3$ has a torsion point of order 2 over ϕ, namely, $(e_1, 0)$. In this case, the associated diophantine equation has one torsion point $(\frac{e_1}{t}, 0)$ of order 2 over $\phi(t)$. Particularly, this gives rise to the torsion subgroup having elements of order 2 over $\phi(t)$: $\{(\infty, \infty), (\frac{e_1}{t}, 0)\} \cong C_2$. This happens when $d = -1, -2, -3, -7, -1(f=2), -3(f=2), -7(f=2)$.

a. If $e_1 \in \mathbb{Q}$, $e_2, e_3 \in \mathbb{C}$ then diophantine equation (1) has a torsion subgroup, having elements of order 2 over $\mathbb{Q}(t)$, but no other torsion subgroup having elements of order 2 over a subset of $\mathbb{C}(t)$. This happens when d = -1, -3, -7.

b) If $e_1 \in \mathbb{Q}$, $e_2, e_3 \in \mathbb{R}$ then diophantine equation (1) has a two element torsion subgroup, having elements of order 2 over $\mathbb{Q}(t)$, and a four element torsion subgroup, having elements of order 2 over $\mathbb{R}(t)$. This happens when d = -2, -1(f=2), -3(f=2), -7(f=2).

2) In the remaining cases, d = -11, -19, -43, -67, -163, -3(f=3) diophantine equation (1) has torsion points of order 2 over at most $Q(t, e_1, e_2, e_3)$.

2.5: Determining the smallest field of containment for the rational solution (x(t),y(t)).

Now that we have described a method of constructing all rational solutions (x(t),y(t)) corresponding to some pair (λ, μ), λ, a complex (or real) multiplier and μ = one of $0, \omega_1, \omega_2, \omega_3 = \omega_1 + \omega_2$; let us conclude this discussion by specifying the smallest field of containment for these solutions - we will include the appropriate method of construction for each case. Details were described earlier.

Case 1. Let $\lambda \in \mathbb{Z}^*$, $\mu = 0$. The rational solutions (x(t),y(t)) take the form

$$x(t) = \frac{p(nu)}{p(u)} \qquad y(t) = \frac{p'(nu)}{p'(u)}$$

These are solutions which correspond to λ, a real multiplier.

Construction. Use the addition formulas as described by statements (11) and (11') with a = n, b = 0; or use the following iterative formula from elliptic function theory.

For $u \neq v$:

$$p(u+v) = \frac{(2p(u)p(v)-(1/2)g_2)(p(u)+p(v))-g_3-p'(u)p'(v)}{2(p(u)-p(v))^2}$$

$$p'(u) = (4p^3(u)-g_2p(u)-g_3)^{1/2}$$

$$p''(u) = 6p^2(u) - (g_2/2) \ .$$

For $u = v$:

$$p(2u) = \frac{[p^2(u)+(g_2/4)]^2+2g_3p(u)}{4p^3(u)-g_2p(u)-g_3} \ .$$

This shows that $(x(t),y(t))$ lie in $\mathbb{Q}(t)$ and in no larger field.

Case 2. Let $\lambda \notin \mathbb{Z}$, $\mu = 0$. The rational solutions $(x(t),y(t))$ take the form

$$x(t) = \frac{p(\lambda u)}{p(u)} \qquad\qquad y(t) = \frac{p'(\lambda u)}{p'(u)}$$

These are solutions which correspond to λ, a complex multiplier.

Construction. Use the addition formulas, successively, in which $(x(t),y(t)) \leftrightarrow \lambda \in \theta_K$, the ring of integers of K, for some a, b. This shows that $(x(t),y(t))$ lie in $Q(t,\lambda)$ and in no larger field.

Case 3. Let $\lambda \in \mathbb{Z}^*$, $\mu \neq 0$. The rational solutions take the form

$$x(t) = \frac{p(nu+\mu)}{p(u)} \qquad y(t) = \frac{p'(nu+\mu)}{p'(u)} \qquad \mu = \omega_1, \omega_2, \omega_3 = \omega_1+\omega_2$$

Construction. Use

$$p(nu+\omega_i) = \frac{e_i p(nu)+(2e_i^2-(1/4)g_2)}{p(nu)-e_i} \quad .$$

If $e_i \in \Phi$, then $(x(t),y(t))$ lie in $\Phi(t)$.

If $e_i \notin \Phi$, then $(x(t),y(t))$ lie in $\Phi(t,e_i)$ for some given i.

Case 4. Let $\lambda \notin \mathbb{Z}$, $\mu \neq 0$. The rational solutions take the form

$$x(t) = \frac{p(\lambda u+\mu)}{p(u)} \qquad y(t) = \frac{p'(\lambda u+\mu)}{p'(u)} \quad , \quad \mu = \omega_1, \omega_2, \omega_3 = \omega_1+\omega_2.$$

Construction. Use the formula of case 3 with $n = \lambda$.

If $e_i \in \Phi$, then $(x(t),y(t))$ lie in $\Phi(t,\lambda)$.

If $e_i \notin \Phi$, then $(x(t),y(t))$ lie in $\Phi(t,\lambda,e_i)$ for some given i.

Section 3: Conclusion

Elliptic curves originally arise because they appear in the integrand for the arc length of an ellipse. Evaluations of such integrals lead one to analyze Legendre's three basic types of such integrals, where, in our case, n equals 3, the degree of f(x) in the elliptic curve, E: $y^2 = f(x)$. Namely, they take the forms (see [9], pg. 41):

$$(1)\quad \underline{\text{First Kind}} = \int \frac{dx}{\sqrt{4x^3-g_2x-g_3}}$$

$$(2)\quad \underline{\text{Second Kind}} = \int -\frac{x\,dx}{\sqrt{4x^3-g_2x-g_3}}$$

$$(3)\quad \underline{\text{Third Kind}} = \int \frac{dx}{(x-a)\sqrt{4x^3-g_2x-g_3}}\,,\ a \in \mathbb{C}\,.$$

The basic results in this paper were consequences of results in elliptic function theory having to do with elliptic integrals of the first kind; especially since the argument, u of the Weierstrass elliptic function, $p(u)$ satisfies

$$u = \int_x^{\infty} \frac{dt}{\sqrt{4t^3-g_2t-g_3}}\,.$$

Although the solutions of the above integrals of the second and third kind deal with the Jacobian elliptic functions, we refer the reader to [9, pg. 151] for determining the expression for the Weierstrass elliptic function $p(u)$ in terms of Jacobian elliptic functions. Specifically, we have the following conclusions:

Let e_1, e_2, e_3 be any three distinct numbers whose sum is zero. Set

$$x = e_3 + \frac{e_1 - e_3}{sn^2(\lambda u; k)}$$

where

$$\lambda^2 = e_1 - e_3 \text{ and } k^2 = \frac{e_2 - e_3}{e_1 - e_3}$$

k = modulus of the Jacobian elliptic functions sn u, cn u, dn u.

We recall the following six identities from Jacobian elliptic function theory:

(1) $\frac{1}{sn\ u} = ns\ u$

(2) $\frac{cn\ u}{sn\ u} = cs\ u$

(3) $\frac{dn\ u}{sn\ u} = ds\ u$

(4) $\frac{d}{du}(sn\ u) = cn\ u\ dn\ u$

(5) $cs^2u + 1 = ns^2u$

(6) $ds^2u + k^2 = ns^2u$

We claim that x satisfies the elliptic curve

$$\left(\frac{dx}{du}\right)^2 = 4(x-e_1)(x-e_2)(x-e_3) .$$

This is the case because

$$\left(\frac{dx}{du}\right) = -2(e_1-e_3)\lambda(sn\lambda u)^{-3}(cn\lambda u)(dn\lambda u) \quad \text{by (4)}$$

$$= -2(e_1-e_3)\lambda(ns\lambda u)(cs\lambda u)(ds\lambda u) \quad \text{by (1), (2), (3).}$$

Then

$$\left(\frac{dx}{du}\right)^2 = 4\lambda^2(e_1-e_3)^2(ns^2\lambda u)(cs^2\lambda u)(ds^2\lambda u)$$

$$= 4\lambda^2(e_1-e_3)^2(ns^2\lambda u)(ns^2\lambda u-1)(ns^2\lambda u-k^2) \quad \text{by (5), (6).}$$

Substituting into $\left(\frac{dx}{du}\right)^2$, the expressions

$$\frac{x-e_3}{e_1-e_3} = ns^2\lambda u \ , \quad \lambda^2 = e_1 - e_3 \ , \ k^2 = \frac{e_2-e_3}{e_1-e_3}$$

we get

$$\left(\frac{dx}{du}\right)^2 = 4(e_1-e_3)(e_1-e_3)^2\left(\frac{x-e_3}{e_1-e_3}\right)\left(\frac{x-e_3}{e_1-e_3} - 1\right)\left(\frac{x-e_3}{e_1-e_3} - \frac{e_2-e_3}{e_1-e_3}\right)$$

$$= 4(x-e_3)(x-e_1)(x-e_2).$$

The theory shows, upon expansion of the right side, that x satisfies the equation.

$$\left(\frac{dx}{du}\right)^2 = 4x^3-g_2x-g_3$$

where g_2, g_3, and the modular invariant j are defined as in the Weierstrass elliptic function theory.

It is with this in mind that we wonder whether the above theory resting on results of Weierstrass elliptic functions can be applied in some modified form to Jacobian elliptic functions as well.

Also, in the process of determining rational solutions over $\mathbb{C}(t)$ to diophantine equation (1), we assumed that diophantine equation (1) was associated with a unique elliptic curve admitting complex multiplication over an imaginary quadratic field having class number one. Suppose we allowed the class number of our

imaginary quadratic field to be greater than one. Then, perhaps, more than one elliptic curve would associate itself with diophantine equation (1). How would the solutions of more than one elliptic curve (although, isogenous curves) interrelate with the rational solutions of our diophantine equation? Would x(t) and y(t) still have the forms

$$x(t) = \frac{p(\lambda u+\mu)}{p(u)} \qquad y(t) = \frac{p'(\lambda u+\mu)}{p'(u)}$$

A more basic question deals with the effect of <u>specific</u> complex values of t on the rank and torsion points of our diophantine equation. We realize that the $p(u)$ series corresponding to $Y^2 = 4X^3 - g_2X - g_3$, for specific g_2, g_3 is unaffected by changes in t. However, for which values of t is diophantine equation (1) an elliptic curve? For which values of t does the rank of diophantine equation (1) decrease? These questions, if investigated, should help us to better understand how and why the above theory works.

Appendix: Preliminary Results on Elliptic Functions and Complex Multiplication.

The following is a summary of the elementary theorems of elliptic function theory and complex multiplication theory, and their respective proofs, as exemplified by this paper. We use the following notation in our discussion of the basic theorems of elliptic function theory:

Lattice, $L = [2\omega_1, 2\omega_2]$, $\tau = \frac{\omega_1}{\omega_2}$ is an imaginary number.

Elliptic function, $f(u)$ is defined over $\mathbb{C}$ and is periodic with respect to L, i.e., for all $z \in \mathbb{C}$, $\omega \in L$, $f(z+\omega) = f(z)$.

Assume $f(u) \neq 0$.

Fundamental period parallelogram, P_α, for $f(u) = [\alpha + 2t_1\omega_1 + 2t_2\omega_2 \mid 0 \leq t_i < 1, i = 1,2]$.

Theorem 1. The number of poles of $f(u)$ in P_α is finite.

Proof. Suppose the number of poles of $f(u)$ in P_α is infinite. By the Bolzano-Weierstrass theorem, this sequence of poles has a limit point. However, any limiting point of poles is an essential singularity of $f(u)$. This means, by the definition of $f(u)$, that $f(u)$ cannot be an elliptic function, since it is not meromorphic.

Theorem 2. The number of zeros of $f(u)$ in P_α is finite.

Proof. Suppose the number of zeros of $f(u)$ in P_α is infinite. Then the number of poles of $1/f(u)$ ($f(u) \neq 0$) is infinite. By the proof of Theorem 1 the limiting point of these poles is an

essential singularity of $1/f(u)$ and is thereby an essential singularity of $f(u)$ - contradicting the fact that $f(u)$ is elliptic.

Theorem 3. The sum of the residues of $f(u)$ at its poles in P_α, is zero.

Proof. Assume $f(u)$ has no poles on the boundary of P_α. For if it did, by Theorem 1, $f(u)$ has a finite number of poles in P_α; we can then translate P_α, without rotation, until no pole of $f(u)$ lies on the boundary. Let C be the contour formed by the edges of P_α, where the corners of P_α are α, $\alpha + 2\omega_1$, $\alpha + 2\omega_2$, $\alpha + 2\omega_1 + 2\omega_2$. The sum of the residues of $f(u)$ at its poles inside C is:

$$\frac{1}{2\pi i}\int_C f(u)\,du = \frac{1}{2\pi i}\left\{\int_\alpha^{\alpha+2\omega_1} f(u)\,du + \int_{\alpha+2\omega_1}^{\alpha+2\omega_1+2\omega_2} f(u)\,du + \int_{\alpha+2\omega_1+2\omega_2}^{\alpha+2\omega_2} f(u)\,du + \int_{\alpha+2\omega_2}^{\alpha} f(u)\,du\right\}$$

Each integration takes place along a straight line path. Change the variable of integration in the second integral on the right by replacing u by $u+2\omega_1$; and in the third integral on the right by replacing u by $u+2\omega_2$. We thereby obtain:

$$\frac{1}{2\pi i}\int_C f(u)\,du = \frac{1}{2\pi i}\left\{\int_\alpha^{\alpha+2\omega_1} f(u)\,du + \int_\alpha^{\alpha+2\omega_2} f(u+2\omega_1)\,du + \int_{\alpha+2\omega_1}^{\alpha} f(u+2\omega_2)\,du + \int_{\alpha+2\omega_2}^{\alpha} f(u)\,du\right\}$$

Since $f(u+2\omega_2) = f(u)$, the first and third integrals differ only in sign as a result of the direction of integration. Similarly, $f(u+2\omega_1) = f(u)$ implies the second and fourth integrals have sum zero. Thus,

$$\int_C f(u)\,du = 2\pi i \cdot [\text{sum of the residues of the poles of } f(u) \text{ inside } C] = 0$$

$\Rightarrow$ the sum of the residues of the poles of $f(u)$, in P_α, is zero.

Theorem 4. If $f(u)$ has no poles in P_α, then $f(u)$ is a constant.

Proof. If $f(u)$ has no poles in P_α it is analytic and therefore bounded inside and on the boundary of P_α. This means there exists a number A such that $|f(u)| < A$ when u is inside or on the boundary of P_α. By the periodicity of $f(u)$, there is some constant A' whereby $|f(u)| < A'$ for all values of u. By Liouville's theorem $f(u)$ is a constant.

Theorem 5. For any elliptic function $f(u)$, the number of zeros in P_α equals the number of poles in P_α.

Proof. Assume again $f(u)$ has no poles or zeros on the boundary C of P_α. By the argument principle we have that

$$\int_C \frac{f'(u)}{f(u)}\,du = 2\pi i(Z-P)$$

where Z equals the total number of zeros of $f(u)$ inside C (finite in number by Theorem 2) counted with multiplicity, and P equals the total number of poles of $f(u)$ inside C (finite in number by Theorem 1) counted with multiplicity. By the periodicity of $f(u)$, we have $f(u+2\omega_1) = f(u)$ and $f(u+2\omega_2) = f(u)$. This implies, after taking derivatives, that $f'(u+2\omega_1) = f'(u)$ and $f'(u+2\omega_2) = f'(u)$. Therefore $f'(u)$ and $f'(u)/f(u)$ have the same periods as $f(u)$. By using the same procedures as in the proof of Theorem 3, we find:

$$\frac{1}{2\pi i}\int_C \frac{f'(u)}{f(u)}\,du =$$

$$\frac{1}{2\pi i}\left\{\int_{\alpha}^{\alpha+2\omega_1}\frac{f'(u)}{f(u)}\,du + \int_{\alpha+2\omega_1}^{\alpha+2\omega_1+2\omega_2}\frac{f'(u)}{f(u)}\,du + \int_{\alpha+2\omega_1+2\omega_2}^{\alpha+2\omega_2}\frac{f'(u)}{f(u)}\,du + \int_{\alpha+2\omega_2}^{\alpha}\frac{f'(u)}{f(u)}\,du\right\} =$$

$$Z - P = 0.$$

Therefore $Z = P$.

Theorem 6. For any elliptic function $f(u)$ and any constant, b, the number of zeros of $f(u)-b$, in P_α, depends only on $f(u)$ and not on b.

Prcof. The function $f(u)-b$ has the same periods as $f(u)$ and $f'(u)$. The poles of $f(u)-b$ are the poles of $f(u)$. By the argument principle the difference between the number of zeros and the number of poles, of $f(u)-b$, inside C is:

$$\frac{1}{2\pi i}\int_C \frac{f'(u)}{f(u)-b}\,du.$$

By using the same procedure as in the proof of Theorem 3, i.e., by dividing the contour into the four parts specified above, we find that, counting multiplicities, the number of zeros of $f(u)-b$ equals the number of poles of $f(u)-b$, which, in turn, equals the number of poles of $f(u)$.

Definition. Assume $f(u)$ has no poles or zeros on the boundary of P_α. The order of $f(u)$ equals the number of poles (or zeros),

counting multiplicities, of f(u) in P_α.

Theorem 7. If f(u) has order less than two, then f(u) is a constant.

Proof. If the order of f(u) is zero, then f(u) has no zeros or poles in P_α, implying by Theorem 4, f(u) is a constant. If the order of f(u) is one, then f(u) has one pole of order one at u = a, in P_α. By Theorem 3, the residue at this pole is zero. Then the coefficient a_{-1}, in the series expansion for f(u):

$$\frac{a_{-1}}{u-a} + \emptyset(u) = f(u)$$

is zero. Hence, u = a is not a pole, but a point of analyticity of f(u). So, f(u) has no poles in P_α, implying by Theorem 4, f(u) is a constant. Therefore, every elliptic function, f(u), has order greater than or equal to two.

In particular, in this paper, we discuss the elliptic function $p(u)$, defined earlier. The Weierstrass function $p(u)$, is an even elliptic function of order two in which each fundamental period parallelogram contains a double pole at the lattice points, L. Other properties about the function $p(u)$ can be found in the references [1], [4], and [9].
We use the following additional notation in our discussion of the two, very basic, theorems of complex multiplication theory:

Elliptic curve E is defined over $\emptyset$ and is described as $Y^2 = 4X^3 - g_2X - g_3$; $E \cong \mathbb{C}/L = P_\alpha$.

Theorem 8. If E admits complex multiplication by λ, then:

(1) λ is integral over $\mathbb{Z}$

(11) $[\mathbb{Q}(\lambda):\mathbb{Q}] = 2$.

Proof. Every elliptic curve, E, is associated with a fundamental period parallelogram, P_α, upon which the elliptic function, $\wp(u)$, is defined. If E admits complex multiplication by λ, then $\lambda L \subset L$, by definition. In particular there exist $a,b,c,d \in \mathbb{Z}$ such that

$$\lambda \cdot 2\omega_1 = a \cdot 2\omega_1 + b \cdot 2\omega_2$$

$$\lambda \cdot 2\omega_2 = c \cdot 2\omega_1 + d \cdot 2\omega_2$$

This implies λ is a root of the polynomial equation

$$\begin{vmatrix} x-a & -b \\ -c & x-d \end{vmatrix} = 0.$$

So, the complex multiplier λ satisfies the integral equation

$$x^2 - (a+d)x + (ad-bc) = 0.$$

Since

$$\lambda = \frac{(a+d) \pm \sqrt{(a+d)^2 - 4(ad-bc)}}{2}$$

we have that λ is of degree two over $\mathbb{Q}$.

Theorem 9. $\mathbb{Q}(\tau) = \mathbb{Q}(\lambda) = K$, when λ is a complex multiplier of L.

Proof. $\lambda 2\omega_2 = c \cdot 2\omega_1 + d \cdot 2\omega_2$ for some integers c,d

$$\lambda = c \cdot (\omega_1/\omega_2) + d$$

$$= c \cdot \tau + d$$

$c \neq 0$, since $\lambda \notin \mathbb{Z}$. In a similar manner, we can write τ in terms of λ. Thus $\Phi(\tau) = \Phi(\lambda)$.

By Theorem 8, λ is an element of the ring of integers $\Phi(\tau)$. Other theorems about complex multiplication can be found in the references [2], [8], and [9].

BIBLIOGRAPHY

1. Appell, P. Principles de la théorie des fonctions elliptiques. Gauther-Villars, Paris, 1922.

2. Borel, A. Seminar on Complex Multiplication , Lecture Notes in Mathematics 21, Springer-Verlag, N.Y. 1966.

3. Cohn, H. Dicphantine Equations over C(t) and Complex Multiplication, Lecture Notes in Mathematics 751, Springer Verlag, N.Y. (1979), pp. 70-81.

4. DuVal, Patrick. Elliptic Functions and Elliptic Curves. Cambridge Univ. Press, London Mathematical Society Lecture Note Series 9, 1973.

5. Hadano, Toshihiro. Conductor of Elliptic Curves with Complex Multiplication and Elliptic Curves of Prime Conductor, Proc. Japan Acad. 51 (1975), pp. 92-95.

6. Mordell, L.J. Diophantine Equations, Academic, London, New York, 1969.

7. Olson, Loren D. Points of Finite Order on Elliptic Curves with Complex Multiplication, Manuscripta Math., 14 (1974), pp. 195-205.

8. Serre, J.P. and Cassels, J.W.S. Complex Multiplication, Algebraic Number Theory Proceedings, Academic, London, 1967, pp. 292-296.

9. Weber, Lehrbuch der Algebra III, Chelsea, New York,1908.