Canad. Math. Bull. Vol. **32** (2), 1989

SOLUTIONS OF SPECIFIC DIOPHANTINE EQUATIONS AND THEIR RELATIONSHIP TO COMPLEX MULTIPLICATION

BY
CLARA WAJNGURT

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

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

and the solutions $(\wp(u), \wp'(u))$ which parametrize the elliptic curve $E, y^2 = 4x^3 - g_2x - g_3$ admitting complex multiplication by λ. We first characterize the form of all rational solutions of diophantine equation (1). The rational solutions are derivable from the subsititutions

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

in which $\mu = 0, \omega_1, \omega_2, \omega_1 + \omega_2 = \omega_3$. 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, $\wp(u)$. Specific examples are finally worked out for the cases $K = \mathbf{Q}(\sqrt{-2})$ and $K = \mathbf{Q}(\sqrt{-7})$.

Introduction. Any elliptic curve E is identified with the group $\mathbf{C}/L$ where L is generated by the periods $2\omega_1, 2\omega_2$, with $\operatorname{Im}(\omega_1/\omega_2) > 0$. The complex analytic endomorphisms of the lattice L which preserve the elliptic curve $E, \alpha(x) = \lambda x, \lambda \in \mathbf{C}, x \in L$ are identified with the multiplication by a complex number, λ, such that $2\omega_1, 2\omega_2$, are elements of L. These endomorphisms of the lattice form a ring which always contain the integers, i.e., $\lambda \in \mathbf{Z}$ – 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 $\mathbf{C}/L$) corresponds to the multiplication of complex numbers $\lambda, \lambda \notin \mathbf{Z}$. By the theory, E is the algebraic curve with a "zero" point (∞, ∞), given by $(X, Y) \in \mathbf{C}$ such that:

$$Y^2 = 4X^3 - g_2X - g_3, g_2^3 - 27g_3^2 \neq 0, Y = \wp'(u), X = \wp(u)$$

Received by the editors February 11, 1988.
AMS Classification: 11G05.

https://doi.org/10.4153/CMB-1989-033-6 Published online by Cambridge University Press

E is thereby associated with the lattice, $L = [2\omega_1, 2\omega_2]$, and the modular invariant j_L, defined by

$$j_L = 2^6 \cdot 3^3 \cdot \frac{g_2^3}{g_2^3 - 27_3^2}.$$

It is a fact that $g_2, g_3 \in \mathbf{Q} \nLeftrightarrow j_L \in Q$. So, in general, End $E \cong \mathbf{Z}$, unless $K = \mathbf{Q}(\omega_1/\omega_2)(= Q(\lambda)$, when λ is a complex multiplier) is an imaginary quadratic field. Also, we find that j_L is an algebraic integer, if E admits complex mutliplications. The degree $[\mathbf{Q}(j_L) : \mathbf{Q}] \leqq h_f$ where f = ring conductor of End E and h = ring class number of $K = \mathbf{Q}(\omega_1/\omega_2)$.

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

$$A(u) = x(\wp(u))\wp(u), B(u) = y(\wp(u))\wp'(u) \tag{2}$$

where $x(\wp(u)), y(\wp(u)) \in$ Rat functions $\{\wp(u)\}$. Set $\wp(u) = t$ in the functions $x(\wp(u)), y(\wp(u))$, thereby obtaining rational functions in t. In (1) we substitute for $(x(t), y(t))$

$$\frac{A(u)}{\wp(u)} = x(t), \frac{B(u)}{\wp'(u)} = y(t), t = \wp(u) \tag{2'}$$

to obtain the elliptic curve

$$4A^3(u) - g_2A(u) - g_3 = B^2(u), g_2^3 - 27g_3^2 \neq 0, j_L \in \mathbf{Q} \tag{3}$$

which is associated with the unique differential of the first kind $d(A(u))/B(u)$. By elliptic function theory $A(u) = \wp(\omega)$, $B(u) = \wp'(\omega)$ for some variable ω, to be determined later. Particularly, we find

$$\frac{d(A(u))}{B(u)} = d\omega = \lambda du \tag{3'}$$

for some $\lambda \in \mathbf{C}^*$. This implies $\omega = \lambda u + +\mu, \mu$ determined modulo the lattice $L = [2\omega_1, 2\omega_2]$ associated with $\wp(u)$. We note that by statement (2) and the symmetry of the elliptic function $\wp(u), A(-u) = A(u)$. Using the above conclusion that $A(u) = \wp(\lambda u + \mu)$, this means $\wp(\lambda u + \mu) = \wp(\lambda(-u) + \mu) = \wp(-\lambda u + \mu)$ modulo L. We get in addition from this that the restriction on μ is $2\mu \equiv 0 \bmod \{2\omega_1, 2\omega_2\}$. This leads us to the following conclusions:

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

$$x(t) = \frac{\wp(\lambda u + \mu)}{\wp(u)}, y(t) = \frac{\wp'(\lambda u + \mu)}{\wp'(u)}, t = \wp(u) \tag{4}$$

https://doi.org/10.4153/CMB-1989-033-6 Published online by Cambridge University Press

In the process, we consider that $X = \wp(u), Y = \wp'(u)$, *parametrize* $Y^2 = 4X^3 - g_2X - g_2X - g_3 = 4(x - e_1)(X - e_2)(x - e_3)e_i \in \mathbf{C}, g_2^3 - 27g_3^2 \neq 0; g_2, g_3 \in \mathbf{Q}$ *and* $\mu = 0, \omega_1, \omega_2, \omega_3$. *This gives us necessary conditions for deriving rational solutions of diophantine equation* (1). *By the following lemma we claim statement* (4) *signifies 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* $\wp(u)$. *Thus, every rational solution* $(x(t), y(t))$ *of diophantine equation* (1) *is intrinsically of the given form described by statement* (4) *if and only if* λ *is a complex (or real) multiplier.*

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.,*

$$x(t) = \frac{\wp(\lambda u + \mu)}{\wp(u)}, y(t) = \frac{\wp'(\lambda u + \mu)}{\wp'(u)}, t = \wp(u), \mu = 0, \omega_1, \omega_2, \omega_3$$

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

$$\lambda y(t) = tx'(t) + x(t) = d(tx(t))/dt \tag{5}$$

Proof. Differentiate $\wp(u)X(t) = \wp(\lambda u + \mu)$ with respect to u. We find

$$\wp(u)X(t)\frac{dt}{du} + X(t)\wp'(u) = \lambda\wp'(\lambda u + \mu).$$

Since $dt/du = \wp'(u)$ the result follows by dividing both sides by $\wp'(u)$. This comes from the fact that the differential $dU = dT/W$ is related to du by $\lambda du = dU$ where λ is one of the complex multipliers and $U = \lambda u + \mu, \mu = 0, \omega_1, \omega_2, \omega_3$.

Corollary 2. *For general solutions* $(x(t), y(t))$ *of diophantine equation* (1), *the* $deg\{tx(t)\} = n$. *Theorem* 2 *enables us to determine the multiplier* λ *if we have already determined the rational solution* $(x(t), y(t))$. *Thus, we observe that every multiplier* λ *is uniquely associated with a rational solution* $(x(t), y(t))$.

Constructing rational solutions by the addition theorems.

Since diophantine equation (1) is a cubic curve over $\mathbf{C}(t)$, 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). The addition theorems of elliptic function theory are applied to diophantine equation (1) in the form:

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

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

https://doi.org/10.4153/CMB-1989-033-6 Published online by Cambridge University Press

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). In the secant formulas we 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 $\mathbf{C}(t)$ of diophantine equation (1) which add in the sense of addition of points on a cubic curve to the sum, over $\mathbf{C}(t)$, (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

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

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

Tangent

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

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

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

The rational solutions of diophantine equation (1) take precisely four forms, each possibility dependent on whether the multiplier ring, $K = \mathbf{Q}(\sqrt{d})$, $d < 0$, $\lambda \in \mathbf{C}^*$ is characterized by

Case A: $d \equiv 2, 3 \pmod 4$, Basis: $[1, \sqrt{d}]$, or
Case B: $d \equiv 1 \pmod 4$, Basis: $[1, (1 + \sqrt{d})/2]$..

We recall, that, in general, the rational solutions are described by

$$x(t) = \frac{\wp(\lambda u + \mu)}{\wp(u)}, y(t) = \frac{\wp'(\lambda u + \mu)}{\wp'(u)}, t = \wp(u), \mu = 0, \omega_1, \omega_2, \omega_3.$$

Case 1 $\lambda \neq 0, \mu = 0$.
The minimal starting set is

$$\textit{Case AB}: (1, 1) \leftrightarrow \lambda = 1, \mu = 0, \text{and}$$

$$\textit{Case A}: \left(\frac{\wp(\sqrt{d}u)}{\wp(u)}, \frac{\wp'(\sqrt{d}u)}{\wp'(u)}\right) \leftrightarrow \lambda = \sqrt{d}, \mu = 0, \text{or}$$

$$\textit{Case B}: \left(\frac{\wp\left(\frac{1+\sqrt{d}}{2}u\right)}{\wp(u)}, \frac{\wp'\left(\frac{1+\sqrt{d}}{2}u\right)}{\wp'(u)}\right) \leftrightarrow \lambda = \frac{1 + \sqrt{d}}{2}, \mu = 0.$$

So all rational solutions of diophantine equation (1) arise from complex (or real) multiplications by the addition formulas as follows:

$$\begin{aligned}
&\mathit{Case\ A}: \ a(1,1)+b\left(\frac{\wp(\sqrt{d}u)}{\wp(u)}, \frac{\wp'(\sqrt{d}u)}{\wp'(u)}\right)\\
&\qquad \leftrightarrow \lambda = a+b\sqrt{d}, a, b \in \mathbf{Z}, \text{norm } \lambda = a^2-b^2d.\\
&\mathit{Case\ B}: \ a(1,1)+b\left(\frac{\wp\left(\frac{1+\sqrt{d}}{2}u\right)}{\wp(u)}, \frac{\wp'\left(\frac{1+\sqrt{d}}{2}u\right)}{\wp'(u)}\right)\\
&\qquad \leftrightarrow \lambda = (a+(b/2))+(b/2)\sqrt{d}, a, b \in \mathbf{Z}\\
&\text{norm}\,\lambda = a^2+ab+\left(\frac{1-d}{4}\right)b^2.
\end{aligned}$$

Case A is exemplified by the quadratic multiplier ring $K = \mathbf{Q}(\sqrt{-2})$, $f = 1$, where the corresponding Weierstrass model is $B^2 = 4A^3 + (-40/3)A + (224/27)$ and whose corresponding diophantine equation is, upon considering the substitution $\wp(u) = (-2t)/3, 2t^3x(t)^3 - 15tx(t) - 14 = y(t)^2(2t^3 - 15t - 14)$. The secant and tangent formulas for this diophantine equation give rise to all rational solutions corresponding to $\lambda \neq 0$, $\mu = 0$ as follows:

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

Case B is exemplified by the quadratic multiplier ring $K = \mathbf{Q}(\sqrt{-7}), f = 1$, where the corresponding Weierstrass model is $B^2 = 4A^3 - 140A - 392$ and whose corresponding diophantine equation is, upon considering the substitution $\wp(u) = t$, $t^3x(t)^3 - 35tx(t) - 98 = y(t)^2(t^3 - 35t - 98)$. The secant and tangent formulas for this diophantine equation give rise to all rational solutions corresponding to $\lambda \neq 0$, $\mu = 0$ as follows:

$$\begin{aligned}
&a(1,1)+b\Biggl(\frac{t^2+(7/2-(1/2)\sqrt{-7})t+(-(7/2)-(21/2)\sqrt{-7}}{\left(\frac{-3+\sqrt{-7}}{2}\right)t(t+(7/2)-(1/2)\sqrt{-7})^2},\\
&\qquad\times\frac{t^2+(7-\sqrt{-7})t+(14+7\sqrt{-7})}{\left(\frac{-5-\sqrt{-7}}{2}\right)(t+(7/2)-(1/2)\sqrt{-7})^2}\Biggr)\\
&\qquad\leftrightarrow \lambda = (a+(b/2))+(b/2)\sqrt{-7}
\end{aligned}$$

Case 2 $\lambda \neq 0, \mu \neq 0$

Since $\mu \neq 0$, we recall by theorem 1 that the possibilities for μ are $\mu = \omega_1, \omega_2, \omega_3$. We determine $\wp(u+\omega_i)$, and therefore $\wp'(u+\omega_i)$ by the following formula from elliptic function theory (see [4], pg. 20).

$$\wp(u+\omega_i) = \frac{e_i\wp(u)+(2e_i^2-(1/4)g_2)}{\wp(u)-e_i}, g_2 \in \mathbf{Q} \tag{6}$$

https://doi.org/10.4153/CMB-1989-033-6 Published online by Cambridge University Press

e_i, described in theorem 1. In particular, $\wp(\lambda u+\omega_i)$ is determined by substituting λu for u on the right side of statement (6). This implies

$$x(t)=\frac{\wp(\lambda u+\omega_i)}{\wp(u)}=\frac{e_i\wp(\lambda u)+(2e_i^2-(g_2/4))}{\wp(u)(\wp(\lambda u)-e_i)},t=\wp(u)$$
$$y(t)=\frac{\wp'(\lambda u+\omega_i)}{\wp'(u)}=\frac{-3e_i^2+(g_2/4)}{(\wp(\lambda u)-e_i)^2},t=\wp(u).$$

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

Case 3 $\lambda=0,\mu=0$

There are no rational solutions associated with this case since $\wp(u)$ and $\wp'(u)$ are both undefined.

Case 4 $\lambda=0,\mu\neq 0$

In this case the rational solutions of diophantine equation (1) are of the form $((e_i/t),0)$ $i=1,2,3$, i.e., the torsion points of order 2 for diophantine equation (1). The case of $g_2,g_3\in Q$ gives rise to particular applications to the thirteen elliptic curves $Y^2=f(x)$ (see [7]) and their associated diophantine equations as developed by this paper.

Determining the smallest field of containment for $(x(t),\ y(t))$.

1) If $\lambda\in\mathbf{Z}^*$, $\mu=0$, $(x(t),\ y(t))$ lie in $\mathbf{Q}(t)$ *and* in no larger field.

2) If $\lambda\in\mathbf{Z}$, $\mu=0$, $(x(t),\ y(t))$ lie in $Q(t,\lambda)$ *and* in no larger field.

3) If $\lambda\in\mathbf{Z}^*$, $\mu\neq 0$.

If $e_i\in\mathbf{Q}$, then $(x(t),\ y(t))$ lie in $\mathbf{Q}(t)$.

If $e_i\notin\mathbf{Q}$, then $(x(t),\ y(t))$ lie in $\mathbf{Q}(t,e_i)$ for some given i.

4) Let $\lambda\notin\mathbf{Z}$, $\mu\neq 0$.

If $e_i\in\mathbf{Q}$, then $(x(t),\ y(t))$ lie in $\mathbf{Q}(t,\lambda)$.

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

Conclusion. Elliptic curves originally arose because their equations 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, $E:y^2=f(x)$. The basic results in this paper are consequences of results in elliptic function theory having to do with elliptic integrals of the first kind. Although the solutions of the integrals of the second and third kind deal with the Jacobian elliptic functions, we refer the reader to [9, p. 151] for determining the expression for the Weierstrass elliptic function $\wp(u)$ in terms of Jacobian elliptic functions. 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. It is possible that this question, if investigated could help us to better understand how and why the above theory works.

https://doi.org/10.4153/CMB-1989-033-6 Published online by Cambridge University Press

References

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

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

3. H. Cohn, *Diophantine Equations over* $\mathbf{C}(t)$ *and Complex Multiplication*, Lecture Notes in Mathematics **751**, Springer-Verlag, N.Y. (1979), pp. 70–81.

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

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

6. Serge Lang, *Elliptic Functions*, Addison-Wesley Publishing Co., Mass., 1973.

7. L. J. Mordell, *Diophantine Equations*, Academic, N.Y., 1969.

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

9. J. P. Serre, *Complex Multiplication, Algebraic Number Theory Proceedings*, Academic, London, 1967, pp. 292–296.

10. Heinrich Weber, *Lehrbuch der Algebra III*, Chelsea, New York, 1908.

Queensborough Community College
Bayside, N.Y. 11364

https://doi.org/10.4153/CMB-1989-033-6 Published online by Cambridge University Press