Elliptic curves over $\mathbb{Q}(i)$

Peter G. Brown[*,**] and Thotsaphon Thongjunthug[*]

Abstract

A study of the diophantine equation $v^2 = 2u^4 - 1$ led the authors to consider elliptic curves specifically over $\mathbb{Q}(i)$ and to examine the parallels and differences with the classical theory over $\mathbb{Q}$. In this paper we present some extensions of the classical theory along with some examples illustrating the results.

The well-known diophantine equation

$$v^2 = 2u^4 - 1\,,$$

has, ignoring signs, only two integer solutions, namely $(u, v) = (1, 1)$ and $(13, 239)$. This is not an easy result to prove (e.g. see [1]).

The change of variable

$$x = \frac{2iv - 2}{u^2}, \qquad y = \frac{-4(v + i)}{u^3}\,,$$

transforms this equation into the elliptic curve

$$y^2 = x^3 + 8x\,.$$

The two integer solutions are transformed as follows:

$$(1, 1) \mapsto (-2 + 2i, -4 - 4i), \qquad (13, 239) \mapsto \left(\frac{2(-1 + 239i)}{13^2}, \frac{-4(239 + i)}{13^3}\right).$$

Thus integer solutions to the diophantine equation become Gaussian rational points on the elliptic curve.

This observation motivated us to look at elliptic curves specifically over $\mathbb{Q}(i)$ to examine the parallels and differences with the classical theory.

Definitions

An *elliptic curve* E (in Weierstrass form) over a field K is an equation of the form

$$y^2 = f(x) = x^3 + Ax + B\,,$$

where $A, B \in K$ and all roots of $f(x)$ are distinct.

Received 11 February 2008; accepted for publication 28 May 2008.
*School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052.
**E-mail: peter@unsw.edu.au

We define $E(L)$ to be the set of ordered pairs

$$\{(x, y) \in L \times L \colon y^2 = f(x)\} \cup \{\infty\},$$

where $L \supseteq K$ is a field. The extra point ∞ is called the *point at infinity.*

It is well known that under a certain operation described geometrically in Figure 1, the set $E(L)$ is an abelian group with ∞ as the identity.

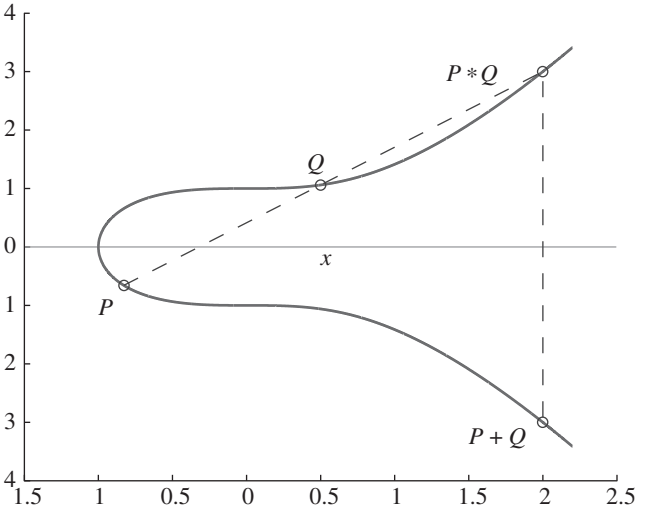

Figure 1.

To *add* points P and Q on the elliptic curve, first we draw a line through the two points. If the line is vertical we define the sum $P + Q$ to be ∞, otherwise, the line will again intersect the curve at a point we will call $P * Q$. Now reflect this point in the x-axis to obtain the point which we will define as $P + Q$. To add P to itself, we take a tangent line at P and use the above. Given two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on an elliptic curve in Weierstrass form, one can easily write down the necessary algebraic formulae for $P + Q$ and for $P + P$. These formulae then become the definition of addition for curves defined over finite and general fields, where the geometric definition has no meaning. Care needs to be taken with fields of characteristic 2 or 3 to avoid division by zero. They will be excluded from our discussion here.

The Lutz–Nagell theorem

A *torsion point* in $E(L)$ is a point of finite order. For elliptic curves over $\mathbb{Q}$, the following theorem (due to Nagell [2], and independently Lutz [3]) gives a simple characterisation of such points.

Theorem 1 (Lutz–Nagell)**.** *Let* $E \colon y^2 = x^3 + Ax + B$ *be an elliptic curve with* $A, B \in \mathbb{Z}$*, and let* $P = (x, y) \in E(\mathbb{Q})$*.*

If P has finite order, then

(1) *both x and y are integers, and*
(2) *either $y = 0$ or $y^2 \mid 4A^3 + 27B^2$.*

Example. Find all torsion points in $E(\mathbb{Q})$ when E is the elliptic curve $y^2 = x^3 + 4$.

Solution. Suppose that $P = (x, y) \in E(\mathbb{Q})$ has finite order. By the Lutz–Nagell theorem, we know that either $y = 0$, or y^2 divides $4A^3 + 27B^2 = 3^3 \cdot 2^4$. Thus the possibilities for y occur in the following list:

$$0, \quad \pm 1, \quad \pm 2, \quad \pm 3, \quad \pm 4, \quad \pm 6, \quad \pm 12\,.$$

Trial and error shows that only $y = \pm 2$ gives x to be an integer. Hence the only possibilities here that need to be checked are $(0, \pm 2)$. Since $(0, -2) = -(0, 2)$, it suffices to check only one point, say, $P = (0, 2)$. By the addition defined above, it can be checked that

$$2P = P + P = (0, -2) = -P\,,$$

hence $3P = \infty$. Thus P and $-P$ have order 3. Therefore the torsion subgroup of $E(\mathbb{Q})$ is

$$\{\infty, (0, 2), (0, -2)\}\,,$$

which is isomorphic to the additive group $\mathbb{Z}/3\mathbb{Z}$.

This theorem can be easily generalised to:

Theorem 2 (Extended Lutz–Nagell theorem)**.** *Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve with $A, B \in \mathbb{Z}[i]$, and let $P = (x, y) \in E(\mathbb{Q}(i))$.*

If P has finite order, then

(1) *both x and y are Gaussian integers, and*
(2) *either $y = 0$ or $y^2 \mid 4A^3 + 27B^2$.*

The proof is obtained by a simple modification of the classical proof (e.g. see [4, pp. 89–196] for details of the classical proof).

The torsion group associated to an elliptic curve cannot be arbitrary. Indeed Mazur [5] showed that the range of such torsion subgroups is very limited.

Theorem 3 (Mazur [5])**.** *If E is an elliptic curve over $\mathbb{Q}$, then the torsion subgroup $E(\mathbb{Q})$ is isomorphic to one of the following 15 groups:*

$$\mathbb{Z}/n\mathbb{Z}, \text{ for } 1 \le n \le 12, n \ne 11,$$
$$(\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2n\mathbb{Z}), \text{ for } 1 \le n \le 4\,.$$

Example. Consider the elliptic curve

$$y^2 + xy - 5y = x^3 - 5x^2\,,$$

which can be transformed into the Weierstrass equation as

$$E\colon y^2 = x^3 - 12987x - 263466\,.$$

Once we consider the torsion subgroup of $E(\mathbb{Q}(i))$, we obtain Table 1.

Table 1.

Order	Points
1	∞
2	$(-21,0)$, $(-102,0)$, $(123,0)$
4	$(-57,\pm 540)$, $(-21-108i,\pm(1296+972i))$, $(33,\pm 810i)$
	$(-237,\pm 3240i)$, $(-21+108i,\pm(1296-972i))$, $(303,\pm 4860)$

Then from this table, it is clear that the torsion subgroup of $E(\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/4\mathbb{Z})$, which is one of the possibilities given by Mazur's theorem. However, the torsion subgroup of $E(\mathbb{Q}(i))$ now becomes $(\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/4\mathbb{Z})$, which is not in Mazur's list.

This is a special case of:

Theorem 4 (Kenku–Momose 1988)**.** *Let F be a quadratic field and E be an elliptic curve over F. Then the torsion subgroup of $E(F)$ is isomorphic to one of the following 26 groups:*

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z}, &\text{ for } 1 \le n \le 18,\ n \ne 17,\\ (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2n\mathbb{Z}), &\text{ for } 1 \le n \le 6,\\ (\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/3n\mathbb{Z}), &\text{ for } n = 1, 2,\\ (\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/4\mathbb{Z}). & \end{aligned}$$

The question as to precisely which torsion subgroups of $E(\mathbb{Q}(i))$ for elliptic curves over $\mathbb{Q}$ can occur is still unresolved. One can also ask the same question for elliptic curves whose coefficients are from $\mathbb{Q}(i)$.

Elliptic curves over $\mathbb{F}_p(i)$, $p \equiv 3 \bmod 4$

The study of elliptic curves over a finite field $\mathbb{F}_p$, p prime, goes back to Gauss.

Theorem 5 (Gauss)**.** *Let E be the elliptic curve*

$$y^2 = x^3 + kx\,,$$

and $p \ne 2$ be a prime such that $p \nmid k$.

If $p \equiv 3 \bmod 4$, then $|E(\mathbb{F}_p)| = p + 1$.

The case $p \equiv 1 \bmod 4$ has also been dealt with, but the answer is not so straightforward.

More generally, one wants to deal with elliptic curves over the finite field $\mathbb{F}_q$, with $q = p^k$, p prime.

The following important result is due to Hasse.

Theorem 6 (Hasse 1933)**.** *Let E be an elliptic curve over the finite field $\mathbb{F}_q$. Then the order of $E(\mathbb{F}_q)$ satisfies the inequality*

$$q + 1 - 2\sqrt{q} \le |E(\mathbb{F}_q)| \le q + 1 + 2\sqrt{q}\,.$$

We take our field now to be $\mathbb{F}_p(i) = \{a + ib \colon a, b \in \mathbb{F}_p\}$ with $p \equiv 3 \bmod 4$. (Note, of course, that $\mathbb{F}_p(i) \cong \mathbb{F}_p$ in the case $p \equiv 1 \bmod 4$.)

This field is isomorphic to $\mathbb{F}_{p^2}$ so Hasse's theorem yields:

$$(p-1)^2 \leq |E(\mathbb{F}_p(i))| \leq (p+1)^2.$$

Returning to the family of elliptic curves in Gauss' result above, we proved:

Theorem 7. *Suppose that E is the elliptic curve of the form*

$$y^2 = x^3 + kx\,,$$

and p is a prime congruent to 3 mod 4 such that $p \nmid k$.

Then $|E(\mathbb{F}_p(i))| = (p+1)^2$, which is the upper bound in Hasse's result.

Proof. The well-known Hasse–Davenport relation (e.g. see [6]) states that if we write $|E(\mathbb{F}_p)| = p + 1 - a$ and $X^2 - aX + p = (X - \alpha)(X - \beta)$ then

$$|E(\mathbb{F}_{p^n})| = p^n + 1 - (\alpha^n + \beta^n)\,.$$

Hence for $p \equiv 3 \bmod 4$, Gauss' result gives $|E(\mathbb{F}_p)| = p + 1$ so $a = 0$ and we write $X^2 + p = (X - i\sqrt{p})(X + i\sqrt{p})$. Hence

$$|E(\mathbb{F}_p(i))| = |E(\mathbb{F}_{p^2})| = p^2 + 1 - ((i\sqrt{p}\,)^2 + (-i\sqrt{p}\,)^2) = (p+1)^2\,.$$

Example. Consider the elliptic curve $y^2 = x^3 + x$ over $\mathbb{F}_3(i)$. A direct calculation gives us Table 2 and thus $|E(\mathbb{F}_3(i))| = 16 = (3+1)^2$.

Table 2.

x	$x^3 + x$	y	Points	Order
0	0	0	$(0, 0)$	2
i	0	0	$(i, 0)$	2
$2i$	0	0	$(2i, 0)$	2
1	2	$\pm i$	$(1, i), (1, 2i)$	4
$1 + i$	2	$\pm i$	$(1 + i, i), (1 + i, 2i)$	4
$1 + 2i$	2	$\pm i$	$(1 + 2i, i), (1 + 2i, 2i)$	4
2	1	± 1	$(2, 1), (2, 2)$	4
$2 + i$	1	± 1	$(2 + i, 1), (2 + i, 2)$	4
$2 + 2i$	1	± 1	$(2 + 2i, 1), (2 + 2i, 2)$	4
∞			∞	1

Mordell–Weil theorem

The group $E(\mathbb{Q})$ of rational points on the elliptic curve E forms an abelian group. In 1922, Mordell [7] showed that this group is finitely generated. This result was generalised by Weil [8]. As a simple consequence of Weil's work, it follows that group $E(\mathbb{Q}(i))$ of Gaussian rational points on the elliptic curve E is also finitely generated.

One of the key tools in Mordell's original proof was his notion of a *height function*, $H(x)$, which attempted to measure how *complicated* a given rational number is.

Mordell defined

$$H(x) = \begin{cases} \max\{|a|, |b|\} & \text{if } x \neq 0,\ x = a/b,\ \gcd(a,b) = 1, \\ 1 & \text{if } x = 0\,. \end{cases}$$

If $P = (x, y) \in E(\mathbb{Q})$ then we can measure its complexity as a rational elliptic point by

$$H(P) = H(x, y) = \begin{cases} 1 & \text{if } P = \infty, \\ H(x) & \text{otherwise.} \end{cases}$$

We can redefine the height function to extend to the Gaussian rationals, as follows:

$$H'(x) = \begin{cases} \max\{|z_1|^2, |z_2|^2\} & \text{if } z \neq 0,\ z = z_1/z_2,\ \gcd(z_1, z_2) = \epsilon, \\ 1 & \text{if } z = 0, \end{cases}$$

where ϵ is a unit in $\mathbb{Z}[i]$ (i.e. one of the numbers $\pm 1, \pm i$).

Then, if $P = (x, y) \in E(\mathbb{Q}(i))$, we define

$$H'(P) = H'(x, y) = \begin{cases} 1 & \text{if } P = \infty, \\ H'(x) & \text{otherwise.} \end{cases}$$

Using this definition, the elementary (but difficult) proof of Mordell can be modified to extend the hypothesis from $\mathbb{Q}$ to $\mathbb{Q}(i)$.

Example. Consider the elliptic curve

$$y^2 = x^3 - 9\,.$$

If we regard this as an elliptic curve over $\mathbb{Q}$, it can be checked that it has a trivial torsion subgroup $\{\infty\}$, and the rank of $E(\mathbb{Q})$ is zero. Thus we have $E(\mathbb{Q}) = \{\infty\}$, that is, there is no rational point (x, y) on this curve.

On the other hand, if we regard this as an elliptic curve over $\mathbb{Q}(i)$, the extended Lutz–Nagell theorem says that the torsion subgroup of $E(\mathbb{Q}(i))$ is

$$T = \{\infty,\ (0, 3i),\ (0, -3i)\} \cong \mathbb{Z}/3\mathbb{Z}\,.$$

It is easy to see that $(2, \pm i) \in E(\mathbb{Q}(i))$. Since $(2, \pm i) \notin T$, they cannot have finite order. Hence we can conclude that

$$E(\mathbb{Q}(i)) \cong (\mathbb{Z}/3\mathbb{Z}) \oplus \mathbb{Z}^r\,,$$

for some integer $r \geq 1$. In other words, there are infinitely many $\mathbb{Q}(i)$-points on this curve. In fact, it can be checked that, for example,

$$\begin{aligned} 2(2, i) &= (-40, -253i)\,, \\ 3(2, i) &= \left(\frac{629}{441}, \frac{22870i}{9261}\right), \\ 4(2, i) &= \left(\frac{-639280}{64009}, \frac{-513439919i}{16194277}\right), \end{aligned}$$

and so on.

Of course, the more interesting question is whether $(0, 3i)$ and $(2, i)$ generate the group $E(\mathbb{Q}(i))$. The techniques used by Mordell can be adapted to answer this question for this curve, but this is beyond the scope of this brief article.

References

[1] Steiner, R. and Tzanakis, N. (1991). Simplifying the solution of Ljunggren's equation, $x^2 + 1 = 2y^4$. *J. Number Theory* **37,** 123–132.

[2] Nagell, T. (1935). Solution de quelque problémes dans la théorie arithmétique des cubiques planes du premier genre. *Wid. Akad. Skrifter Oslo I* **1**.

[3] Lutz, E. (1937). Sur l'équation $y^2 = x_2 - Ax - B$ dans les corps p-adiques. *J. Reine Agnew. Math.* **177,** 237–247.

[4] Washington, L.C. (2003). *Elliptic Curves: Number Theory and Cryptography.* (Series *Discrete Mathematics and its Applications.*) CRC Press, Boca Raton, FL.

[5] Mazur, B. (1977). Modular curves and the Eisenstein ideal. *Inst, Hautes Etudes Sci. Publ. Math.* **47,** 33–186.

[6] Ireland, K.F. and Rosen, M.I. (1972). *Elements of Number Theory.* Bogden & Quigley, Tarrytown-on-Hudson, NY.

[7] Mordell, L.J. (1922). On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Camb. Philos. Soc.* **21,** 179.

[8] Weil, A. (1929). L'arithmetique sur les courbes algebriques. *Acta Math.* **42,** 281–315. (Reprinted in Volume 1 of his collected papers, ISBN 0387093305.)