Pacific Journal of Mathematics

CONSTRUCTION OF ELLIPTIC CURVES WITH NONINTEGER TORSION POINTS AND NONCYCLIC TORSION GROUPS

SUMI JEONG AND HWASIN PARK

Volume 244 No. 2 February 2010

PACIFIC JOURNAL OF MATHEMATICS
Vol. 244, No. 2, 2010

CONSTRUCTION OF ELLIPTIC CURVES WITH NONINTEGER TORSION POINTS AND NONCYCLIC TORSION GROUPS

SUMI JEONG AND HWASIN PARK

We study elliptic curves in Weierstrass form (with integer coefficients) that have noninteger torsion points over $\mathbb{Q}$. After putting the curves in certain normal forms, we find conditions on their coefficients characterizing when the torsion group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$, for each $N = 1, 2, 3, 4$.

1. Introduction and main results

Let E be an elliptic curve given by the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{Z}, \tag{1-1}$$

and assume E has a noninteger torsion point in the projective plane $\mathbb{P}^2(\mathbb{Q})$. Then E has one of the following expressions, up to a translation $(x, y) \mapsto (x-\alpha, y-\beta)$ with $\alpha, \beta \in \mathbb{Z}$:

$$E_1 : y^2 + xy = x^3 + 4(a - 4b)x^2 + ax + b,$$
$$E_2 : y^2 + xy + y = x^3 + 2(2a - 8b - 1)x^2 + ax + b.$$

(See Theorem 1.) Here $a, b \in \mathbb{Z}$. The curve E_1 has a noninteger torsion point at $(-\frac{1}{4}, \frac{1}{8})$, and E_2 one at $(-\frac{1}{4}, -\frac{3}{8})$.

If a curve of the form E_1 or E_2 has a noninteger point in $\mathbb{P}^2(\mathbb{Q})$ apart from $(-\frac{1}{4}, \frac{1}{8})$ or $(-\frac{1}{4}, -\frac{3}{8})$, respectively, that point has infinite order, so the curve has rank at least 1. In Section 2 we give explicit examples.

Since E_1 and E_2 have a 2-torsion point, we may ask for what choices of the coefficients the torsion subgroup is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$, for $N = 1, 2, 3$, or 4 (higher values of N being excluded by [Mazur 1977]). In Sections 3 and 4, we give criteria for determining whether a curve of the form E_1 or E_2 has such a noncyclic torsion subgroup, and construct all possible families of elliptic curves with noninteger torsion points and a noncyclic torsion subgroup. Specifically:

MSC2000: 11G05, 14G05.
Keywords: elliptic curve.

- Let m, n be integers of the same parity and set

$$E_{11} : y^2 + xy = x^3 + 2(m+n)x^2 + \bigl(4mn + \tfrac{1}{2}(m+n)\bigr)x + mn \tag{1-2}$$

  as a particular case of E_1. The torsion group of such curves contains a $(\mathbb{Z}/2\mathbb{Z})^2$ (Theorem 8). We also construct a similar family based on E_2 (Theorem 13).

- No curve E_2 can have torsion subgroup $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ (Theorem 14). For the case of E_1, we construct curves with these torsion groups as follows:

  (a) Assume that k, s are integers, with $s > 0$. If we choose

$$m = -k - 2k^2 \quad \text{and} \quad n = m + 2s^2, \tag{1-3}$$

  then E_{11} has a torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ (Theorem 10).

  (b) Let $(v, w, \square)$ be a primitive Pythagorean triple with v even, and let t be a nonnegative integer. For $s = v^2(4t+1)/4$ and $k = (w^2(4t+1)-1)/4$ or $s = v^2(4t+3)/4$ and $k = -(w^2(4t+3)+1)/4$, the elliptic curve E_{11} defined by (1-2) and (1-3) has torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ (Theorem 15).

  Elliptic curves with torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ have been classified (see [Campbell and Goins 2004, Theorem 6.2], for example). They all can be written in the form just given (Remark 16).

- We construct elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ in Theorems 12(d) and 14(c). Via coordinate transformations these curves take the form

$$y^2 = \Bigl(x + \frac{(s+t)^2}{4}\Bigr)\Bigl(x + \frac{(s-t)^2}{4}\Bigr)\Bigl(x + \frac{(s+t)^2(s-t)^2}{16t^2}\Bigr)$$

  where s, t are integers satisfying $s \neq t, -3t$, $t \mid s^2$ and $s \equiv t \equiv 1$ or $3 \pmod 4$.

2. Elliptic curves with noninteger torsion points in $\mathbb{P}^2(\mathbb{Q})$ and rank ≥ 1

Given an elliptic curve in Weierstrass form (1-1), we can replace y by $y - a_1x/2$ if a_1 is even, or by $y - (a_1-1)x/2$ if a_1 is odd, to obtain an isomorphic curve in Weierstrass form with $a_1 = 0$ or $a_1 = 1$.

By the Lutz–Nagell theorem, if $a_1 = 0$ and $P = (x_P, y_P)$ is a rational torsion point, then x_P and y_P are integers. Because we are interested in finding elliptic curves with *noninteger* torsion points, we therefore restrict our attention to the case $a_1 = 1$; that is, our curve has the form

$$E' : y^2 + xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad \text{where } a_2, a_3, a_4, a_6 \in \mathbb{Z}. \tag{2-1}$$

Theorem 1. *Assume the curve E' in (2-1) has noninteger torsion points. Then, up to a coordinate translation $(x, y) \mapsto (x-\alpha, y-\beta)$ with $\alpha, \beta \in \mathbb{Z}$, the curve is of* *one of the following forms, where a, b are integers*:

$$\begin{aligned} E_1 &: y^2+xy=x^3+4(a-4b)x^2+ax+b, \\ E_2 &: y^2+xy+y=x^3+2(2a-8b-1)x^2+ax+b. \end{aligned} \tag{2-2}$$

Proof. By the Lutz–Nagell theorem, a noninteger torsion point P of E' in $\mathbb{P}^2(\mathbb{Q})$ must have order two and coordinates $(x_P, y_P)=(m/2^2, n/2^3)$, with $m, n \in \mathbb{Z}$. From $2P=O$, the group law gives

$$2y_P+x_P+a_3=0, \tag{2-3}$$

hence $n+m=-4a_3$. This implies $n+m\equiv 0 \pmod 4$. We thus have the following possibilities for P, where α and β are integers:

- $m\equiv 0 \pmod 4$, $n\equiv 0 \pmod 4$ $\implies$ $P=(\alpha, \beta+\frac{1}{2})$.
- $m\equiv 1 \pmod 4$, $n\equiv 3 \pmod 4$ $\implies$ $P=(\alpha+\frac{1}{4}, \beta-\frac{1}{8})$ or $P=(\alpha+\frac{1}{4}, \beta+\frac{3}{8})$.
- $m\equiv 2 \pmod 4$, $n\equiv 2 \pmod 4$ $\implies$ $P=(\alpha+\frac{1}{2}, \beta\pm\frac{1}{4})$.
- $m\equiv 3 \pmod 4$, $n\equiv 1 \pmod 4$ $\implies$ $P=(\alpha-\frac{1}{4}, \beta+\frac{1}{8})$ or $P=(\alpha-\frac{1}{4}, \beta-\frac{3}{8})$.

By a coordinate translation, we can assume $\alpha=0$ and $\beta=0$, so the possibilities for P after this reduction are $(0, \frac{1}{2})$, $(\frac{1}{2}, \pm\frac{1}{4})$, $(\pm\frac{1}{4}, \mp\frac{1}{8})$ and $(\pm\frac{1}{4}, \pm\frac{3}{8})$. However, not all them can occur. If $P=(\frac{1}{2}, \frac{1}{4})$, for example, the equality $2y_P+x_P+a_3=0$ gives $a_3=-1$, so $\frac{1}{16}+\frac{1}{8}-\frac{1}{4}=\frac{1}{8}+\frac{1}{4}a_2+\frac{1}{2}a_4+a_6$, which is impossible for $a_2, a_4, a_6\in\mathbb{Z}$. A similar calculation excludes all but two cases:

- $P=(-\frac{1}{4}, \frac{1}{8}) \implies a_3=0,\ a_2=4a_4-16a_6$,
- $P=(-\frac{1}{4}, -\frac{3}{8}) \implies a_3=1,\ a_2=4a_4-16a_6-2$.

Setting $a=a_4$ and $b=a_6$ yields the forms in (2-2). □

Remark 2. It follows that, if an elliptic curve of the form E_1 or E_2 has a noninteger point in $\mathbb{P}^2(\mathbb{Q})$ other than $(-\frac{1}{4}, \frac{1}{8})$ or $(-\frac{1}{4}, -\frac{3}{8})$, respectively, that point contributes to the rank of the curve. Similarly, if a curve is *not* isomorphic to either E_1 or E_2 and has a noninteger rational point, this point contributes to the rank, since it is not a torsion point.

Remark 3. The condition (2-3) in the proof of Theorem 1 being also sufficient for P to have order 2, any curve of the form (2-2) with integer a, b — so long as it is nonsingular — has a point of order 2 with coordinates $(-\frac{1}{4}, \frac{1}{8})$ (in the case of E_1) or $(-\frac{1}{4}, -\frac{3}{8})$ (for E_2).

Theorem 4. *Consider the elliptic curve $E_1 : y^2+xy=x^3+4(a-4b)x^2+ax+b$, where $a, b\in\mathbb{Z}$. If $p/q\in\mathbb{Q}$ is the x-coordinate of a point in $E_1(\mathbb{Q})$, where p, q are relatively prime integers with $q>0$, then q is a square. Further, if $q=4$, then $p\equiv 3 \pmod 4$.*

Proof. Setting $x = p/q$ in the equation for E_1, we see y is rational if and only if

$$q(4p+q)(p^2+4apq-16bpq+4bq^2) \text{ is a square,} \tag{2-4}$$

or equivalently, with $q = q'r^2$, where $r \in \mathbb{Z}$ and q' is a square-free positive integer,

$$q'(4p+q)(p^2+4apq-16bpq+4bq^2) \text{ is a square.} \tag{2-5}$$

Assume this is the case. Then $q' \mid (4p+q)(p^2+4apq-16bpq+4bq^2)$, which is the same as $q' \mid 4p^3$. But $q' \nmid p^3$, since $\gcd(p,q) = 1$, so we get $q' = 1$ or $q' = 2$. If $q' = 2$, then p is odd and $(2p+r^2)(p^2+8apr^2-32bpr^2+16br^4)$ is a square, by (2-5). But this cannot be so, because this expression is congruent (mod 4) to $(2p+r^2)p^2 \equiv (2+r^2)\cdot 1 \equiv 2$ or 3. This contradiction shows that $q' = 1$; that is, q is a square.

If $q = 4$, again p is odd and (2-5) implies that $(p+1)(p^2+16ap-64bp+64b)$ is a square. This reduces (mod 4) to $(p+1)p^2 \equiv p+1$. Hence $p \equiv 3 \pmod 4$. □

We can use Remark 2 and Theorem 4 to construct a family of elliptic curves with rank at least 1.

Example 5. For $k, t \in \mathbb{Z}$, consider the elliptic curve

$$E : y^2 + xy = x^3 - (16k^2+12k+16t)x^2 + (12k^2+9k+8t)x + (4k^2+3k+3t).$$

$E(\mathbb{Q})$ contains the point $\left(\frac{3}{4}, \frac{1}{8}(3+16k)\right)$ and its additive inverse $\left(\frac{3}{4}, \frac{1}{8}(-9-16k)\right)$; being noninteger and distinct from $(-\frac{1}{4}, \frac{1}{8})$, these points have infinite order. Hence the curve has rank at least 1.

To see how the example is obtained, we need only consider the conditions on $a, b \in \mathbb{Z}$ such that E_1 in Theorem 4 has a rational point (x, y) with $x = \frac{3}{4}$. Substitution gives $y = \frac{1}{8}(-3 \pm 2\sqrt{9+48a-128b})$; that is, we must find conditions on a, b ensuring that $9+48a-128b = A^2$ for some $A \in \mathbb{Z}$. Since $16(3a-8b) = A^2-9$, we have $16 \mid (A^2-9)$, or, upon replacing A by $-A$ if necessary, $A \equiv 3 \pmod 8$. Put $A = 8k+3$ for some $k \in \mathbb{Z}$; then $3a-8b = 4k^2+3k$. Since $(3, 8) = 1$, we can write $a = 3(4k^2+3k)+8t$ and $b = (4k^2+3k)+3t$ for some $t \in \mathbb{Z}$. We find the value $8k+3$ for the radical and hence the values of y. Working backwards, or simply checking by substitution, we see that any $k, t \in \mathbb{Z}$ will work.

Theorem 6. *Consider the elliptic curve* $E_2 : y^2+xy+y = x^3+2(2a-8b-1)x^2+ax+b$, *where* $a, b \in \mathbb{Z}$. *If* $p/q \in \mathbb{Q}$ *is the* x*-coordinate of a point in* $E_2(\mathbb{Q})$, *where* p, q *are relatively prime integers with* $q > 0$, *then* q *is a square. Further, if* $q = 4$, *then* $p \equiv 3 \pmod 4$.

The proof is similar to that of Theorem 4. Moreover, a reasoning similar to that used to justify Example 5 gives rise to our second example family:

Example 7. Consider the elliptic curve

$$E : y^2+xy+y = x^3-(2+4k+16k^2+16t)x^2+(12k^2+3k+8t)x+(4k^2+k+3t),$$

where $k, t \in \mathbb{Z}$. It has noninteger points $\left(\frac{3}{4}, \frac{1}{8}(-5+16k)\right)$, $\left(\frac{3}{4}, \frac{1}{8}(-9-16k)\right)$ distinct from $(-\frac{1}{4}, -\frac{3}{8})$, so $E(\mathbb{Q})$ has rank at least 1.

We now turn to the torsion groups of the curves E_1 and E_2. We know from Remark 3 that there is always a point of order 2; we wish to find conditions on the coefficients a and b that characterize when the torsion group is noncyclic — which, by [Mazur 1977], means isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$, for $N = 1, 2, 3, 4$.

3. Torsion subgroups on $E_1 : y^2 + xy = x^3 + 4(a - 4b)x^2 + ax + b$

Recall that E_1 has a torsion point of order 2 at $(-\frac{1}{4}, \frac{1}{8})$ so long as it is nonsingular, a condition that boils down to $(a-4b)^2-b \neq 0$, since the discriminant of E_1 factors as $(1-16a+128b)^2((a-4b)^2-b)$, and the square factor is clearly nonzero.

Theorem 8. *Consider the curve E_{11} with equation (1-2), obtained as a particular case of E_1 with coefficients $a = 4mn + \frac{1}{2}(m+n)$ and $b = mn$, where m and n are integers satisfying $m \equiv n \pmod 2$ and $m < n$. The 2-torsion subgroup of E_{11} is $E_{11,\mathrm{tors}}(\mathbb{Q})[2] = \{O, (-\frac{1}{4}, \frac{1}{8}), (-2m, m), (-2n, n)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

All other curves E_1 not of this form have $E_{1,\mathrm{tors}}(\mathbb{Q})[2] = \{O, (-\frac{1}{4}, \frac{1}{8})\} \cong \mathbb{Z}/2\mathbb{Z}$.

Proof. Let E_1 have a torsion point P of order 2 other than $(-\frac{1}{4}, \frac{1}{8})$. From the proof of Theorem 1, and especially (2-3), we know that P has the form $(q/4, -q/8)$ for $q \in \mathbb{Z}$. From the curve's equation we get $(1+q)(q^2+16(a-4b)q+64b) = 0$. But $q \neq -1$ by assumption, so

$$q = -8(a-4b) \pm 8\sqrt{(a-4b)^2-b}. \tag{3-1}$$

That is, $(a-4b)^2 - b = A^2$ for some integer A, which must be nonzero by the observation at the start of this section. Setting $B = a - 4b$, $m = B - A$ and $n = B + A$, so that $b = B^2 - A^2 = mn$ and $a = 4mn + (m+n)/2$, we obtain the equation of E_{11} in the theorem, with the side conditions on m and n. (We know that $m \neq n$ since $A \neq 0$, and we can interchange m and n if necessary to ensure that $m < n$.)

This shows the last assertion of the theorem, and confirms that there cannot be more than three points of order 2, since there are only two choices of q in (3-1). There remains to note that for any m and n as in the statement of the theorem (equivalently, for any integers A, B with $A \neq 0$) we do indeed get torsion points of order 2 via (3-1), arising from $q = -8m$ and $q = -8n$. □

We next recall a classical result; see for example [Knapp 1992, Theorem 4.2].

Lemma 9. *Consider the elliptic curve*

$$E : y^2 = (x - x_1)(x - x_2)(x - x_3). \tag{3-2}$$

For $(x, y) \in E(\mathbb{Q})$, there exists $P \in E(\mathbb{Q})$ with $2P = (x, y)$ if and only if $x - x_1$, $x - x_2$, $x - x_3$ are squares.

Theorem 10. *Let k and s be integers, with $s > 0$. If the curve E_{11} of Theorem 8 has coefficients $m = -k - 2k^2$ and $n = -k - 2k^2 + 2s^2$, then it has a torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.*

Proof. The coordinate change $y = \eta - x/2$ followed by $(x, \eta) = (X/4, Y/8)$ transforms E_{11} into the curve

$$E'_{11} : Y^2 = (X + 1)(X + 8m)(X + 8n). \tag{3-3}$$

The points $(-\frac{1}{4}, \frac{1}{8})$, $(-2m, m)$ and $(-2n, n)$ of order 2 in $E_{11}(\mathbb{Q})$ correspond to $(-1, 0)$, $(-8m, 0)$ and $(-8n, 0)$ in $E'_{11}(\mathbb{Q})$. We now ask which, if any, of these points can be the double of some point P in $E'_{11}(\mathbb{Q})$.

If $2P = (-1, 0)$, the differences $-1 - (-1)$, $-1 - (-8m)$ and $-1 - (-8n)$ must be squares, by Lemma 9. But $8m - 1$ is certainly not a square, because it has residue 3 (mod 4). Therefore $(-1, 0)$ is not a double. Similarly, $(-8n, 0)$ is not a double because $-8n - (-8m) < 0$ is not a square. Finally $(-8m, 0)$ is a double if and only if $-8m - (-1)$ and $-8m - (-8n)$ are squares; that is, if and only if $8(n - m) = S^2$ and $1 - 8m = K^2$, where S, K are integers. Clearly $S \equiv 0 \pmod 4$ and K is odd; by interchanging K and $-K$ we can ensure that $K \equiv 1 \pmod 4$. So $E'_{11}(\mathbb{Q})$, and hence also $E_{11}(\mathbb{Q})$, has torsion points of order 4 if and only if

$$n - m = 2s^2 \text{ with } s \in \mathbb{Z},\ s > 0 \quad\text{and}\quad 1 - 8m = (4k + 1)^2 \text{ with } k \in \mathbb{Z},$$

or equivalently if $m = -k - 2k^2$ and $n = -k - 2k^2 + 2s^2$ for $k, s \in \mathbb{Z}$ with $s > 0$. □

Remark 11. Here is the explicit form of the points of order 4 in E'_{11}:

$$\begin{cases} P_1 = \big(4(2k + 4k^2 - s(1 + 4k)),\ \ 4s(1 + 4k)(1 + 4k - 4s)\big) \\ P_2 = \big(4(2k + 4k^2 - s(1 + 4k)), -4s(1 + 4k)(1 + 4k - 4s)\big) \\ P_3 = \big(4(2k + 4k^2 + s(1 + 4k)),\ \ 4s(1 + 4k)(1 + 4k + 4s)\big) \\ P_4 = \big(4(2k + 4k^2 + s(1 + 4k)), -4s(1 + 4k)(1 + 4k + 4s)\big) \end{cases} \tag{3-4}$$

We now recapitulate and complement our results for E_1, giving criteria for the occurrence of each torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $n = 1, 2, 3, 4$.

Theorem 12. *Consider the elliptic curve $E_1 : y^2 + xy = x^3 + 4(a - 4b)x^2 + ax + b$, where $a, b \in \mathbb{Z}$. and recall that $(-\frac{1}{4}, \frac{1}{8})$ is a point of order 2 in $E_1(\mathbb{Q})$.*

(a) *$E_1(\mathbb{Q})$ has a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ if and only if the equation $t^2 - 2(a - 4b)t + b = 0$ in t has two integer solutions $m < n$, in which case E_1 has the form E_{11} of (1-2): $y^2 + xy = x^3 + 2(m+n)x^2 + \big(4mn + \frac{1}{2}(m+n)\big)x + mn$.*

(b) *Assuming the condition in (a) is met, $E_{11}(\mathbb{Q})$ has a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ if and only if $1-8m$ and $\frac{1}{2}(n-m)$ are square integers.*

(c) *In the situation of (b), the full torsion group is $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ if and only if*

$$\sqrt{\frac{n-m}{2}}\left(4\sqrt{\frac{n-m}{2}}+\sqrt{1-8m}\right)\ \text{and}\ \sqrt{1-8m}\left(4\sqrt{\frac{n-m}{2}}+\sqrt{1-8m}\right) \tag{3-5}$$

are square integers.

(d) *Assuming the condition in (a) is met, the full torsion group is $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ if and only if there exist integers α,β such that $|\alpha|<\beta$, $\gamma:=-\alpha\beta/(\alpha+\beta)$ is an integer, $m=\frac{1}{8}(\alpha^2-\gamma^2+1)$, and $n=\frac{1}{8}(\beta^2-\gamma^2+1)$. In this situation the points of order 3 have x-coordinate $\frac{1}{4}(\gamma^2-1)$; moreover γ is odd and $\beta\equiv\alpha\equiv 0 \pmod 4$.*

Proof. Part (a) is just a restatement of Theorem 8, apart from the easily checked equivalence between the conditions $a=4mn+\frac{1}{2}(m+n)$ and $b=mn$ in that theorem and m,n being the roots of the quadratic equation $t^2-2(a-4b)t+b=0$.

(b) If $1-8m$ and $(n-m)/2$ are squares, the quantities $s=\sqrt{(n-m)/2}$ and $k=(-1+\sqrt{1-8m})/4$ or $k=(-1-\sqrt{1-8m})/4$ satisfy the conditions of Theorem 10. (We choose whichever definition of k yields an integer; note that $\sqrt{1-8m}$ is odd.) Therefore in this situation E_{11} has a torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$. Conversely, if E_{11} has a torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$, we have $m=-k-2k^2$ and $n=-k-2k^2+2s^2$ for some integers k,s with $s>0$.

(c) Let s and k be as above, and recall the short form E'_{11} of the curve given in (3-3). We ask when the points P_1, P_2, P_3, P_4 of order four listed in (3-4) are doubles. Consider first the condition imposed by Lemma 9 for P_1 to be a double. It is that the following three differences be squares:

$$\begin{aligned}
4(2k+4k^2-s(1+4k))+1 \quad &= (1+4k)(1+4k-4s),\\
4(2k+4k^2-s(1+4k))+8m &= -4s(1+4k),\\
4(2k+4k^2-s(1+4k))+8n \ &= -4s(1+4k-4s).
\end{aligned}$$

Clearly if any two are squares, so is the third. We discard the middle line and rewrite the other two right-hand sides in terms of m and n, using the expressions in (b). We must take the minus sign in $k=(-1\pm\sqrt{1-8m})/4$, since s is positive and $-4s(1+4k)$ is a square. It follows that the condition for P_1 to be a double is that the quantities in (3-5) be square integers. The same holds for P_2, since it has the same x-coordinate as P_1.

A similar argument shows that the condition on the integers $s>0$ and k for P_3 (or P_4) to be a double is that $s(1+4k+4s)$ and $(1+4k)(1+4k+4s)$ be squares. Substituting $k=(-1+\sqrt{1-8m})/4$ and s leads to the same expressions (3-5) in terms of m and n. Thus there is a point of order 8 in the curve if and only if both quantities in (3-5) are square integers. (Because of the different relationship between k and m in each case, P_1 and P_2 being doubles is mutually exclusive with P_3 and P_4 being doubles, as expected from the structure of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.)

(d) Assume the curve has a point of order 3, and let (X_P, Y_P) be its coordinates in the alternate equation (3-3) introduced in the proof of Theorem 10. Because this point is the double of a generator of $\mathbb{Z}/6\mathbb{Z}$, we can apply Lemma 9 to conclude that $A := X_P + 8m$, $B := X_P + 8n$, $G := X_P + 1$ are all square integers.

Meanwhile, the standard algebraic constraint for a point on an elliptic curve of the form (3-2) to have order three (easy to derive using the characterization of such a point as an inflection point) amounts in this case to

$$4ABG(A+B+G) - (BG+AB+AG)^2 = 0. \tag{3-6}$$

If we let α, β, γ be the nonnegative square roots of A, B, G (note that $\alpha < \beta$ since $m < n$), we can write the left-hand side of (3-6) as

$$(\alpha\beta+\beta\gamma+\alpha\gamma)(-\alpha\beta+\beta\gamma+\alpha\gamma)(\alpha\beta-\beta\gamma+\alpha\gamma)(\alpha\beta+\beta\gamma-\alpha\gamma),$$

so one of these factors vanishes. By changing the sign of α and/or γ we can ensure that $\alpha\beta+\beta\gamma+\alpha\gamma = 0$, while β remains positive and greater than $|\alpha|$. Thus $\gamma = -\alpha\beta/(\alpha+\beta)$. Substitution also gives, successively,

$$X_P = \gamma^2 - 1, \quad m = \tfrac{1}{8}(\alpha^2-\gamma^2+1), \quad n = \tfrac{1}{8}(\beta^2-\gamma^2+1).$$

Recalling that the x-coordinate in E_{11} is related to the X-coordinate in E'_{11} by $x = X/4$, we deduce that $x = \frac{1}{4}(\gamma^2-1)$. The divisibility conditions on γ, α, β follow since x, m, n are integers. This concludes one direction of the proof.

The other direction is a matter of checking (using the same algebra) that, given integers α, β, γ with $\gamma = -\alpha\beta/(\alpha+\beta)$, $m = \frac{1}{8}(\alpha^2-\gamma^2+1)$, and $n = \frac{1}{8}(\beta^2-\gamma^2+1)$, the points on E_{11} with $x = \frac{1}{4}(\gamma^2-1)$ have order 3. $\square$

4. Torsion subgroups on $E_2 : y^2 + xy + y = x^3 + 2(2a-8b-1)x^2 + ax + b$

Recall that E_2 has a torsion point of order 2 at $(-\frac{1}{4}, -\frac{3}{8})$ so long as it is nonsingular, a condition equivalent to $(a-4b)^2 - a + 3b \neq 0$, since the discriminant of E_2 factors as $(25-16a+128b)^2((a-4b)^2-a+3b)$, and the square factor is clearly nonzero.

Theorem 13. *Consider the curve*

$$E_{22} : y^2 + xy + y = x^3 + 2(m+n)x^2 + \big(4mn + \tfrac{1}{2}(m+n-1)\big)x + mn - \tfrac{1}{4}$$

*obtained as a particular case of E_2 with coefficients $a = 4mn + \frac{1}{2}(m+n) - \frac{1}{2}$ and $b = mn - \frac{1}{4}$, where m and n are **half**-integers (that is, $2m, 2n$ are odd integers)* *satisfying* $m-n\equiv 0 \pmod 2$ *and* $m<n$. *Then* E_{22} *does not have torsion points of order* 4, *and the* 2*-torsion subgroup of* E_{22} *is*

$$E_{22,\mathrm{tors}}(\mathbb{Q})[2]=\bigl\{O,\,(-\tfrac14,-\tfrac38),\,\bigl(-2m,m-\tfrac12\bigr),\,\bigl(-2n,n-\tfrac12\bigr)\bigr\}\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}.$$

All other curves E_2 *not of this form have* $E_{2,\mathrm{tors}}(\mathbb{Q})[2]=\bigl\{O,(-\tfrac14,-\tfrac38)\bigr\}\cong\mathbb{Z}/2\mathbb{Z}$.

Proof. Assume that E_2 has a torsion point P of order 2 other than $(-\frac14,-\frac38)$, and write $P=\bigl(q/4,-q/8-\frac12\bigr)$ with $q\in\mathbb{Z}$. From the equation of E_2 we obtain $(1+q)(q^2+8q(2a-8b-1)+16(4b+1))=0$, so

$$q=-4(2a-8b-1)\pm 4\sqrt{(2a-8b-1)^2-(4b+1)}. \tag{4-1}$$

That is, $(2a-8b-1)^2-(4b+1)=A^2$ for some even integer A, which must be nonzero by the observation at the start of this section (note that the radicand in (4-1) equals $(a-4b)^2-a+3b$). Setting $B=2a-8b-1$, $m=\frac12(B+A)$ and $n=\frac12(B-A)$, so that $b=\frac14(B^2-A^2-1)=mn-\frac14$ and $a=\frac12(B+8b+1)=\frac12(m+n)+(4mn-1)+\frac12$, we obtain the equation of E_{22} in the theorem, with the side conditions on m and n.

This shows the last assertion of the theorem, and also that there cannot be more than three points of order 2, since there are only two choices of q in (4-1). Further, for any m and n as in the statement of the theorem (equivalently, for any nonzero even integer A and any odd integer B) we do indeed get torsion points of order 2 via (4-1), arising from $q=-8m$ and $q=-8n$.

There remains to show that $E_{22}(\mathbb{Q})$ has no torsion of order 4. To do this, apply the coordinate change $y=\eta-(x+1)/2$ followed by $(x,\eta)=(X/4,Y/8)$. This transforms E_{22} into the curve

$$E'_{22}: Y^2=(X+1)(X+8m)(X+8n), \tag{4-2}$$

which is the same as E'_{11} of (3-3). The points of order two listed above map become $(-1,0)$, $(-8m,0)$, and $(-8n,0)$. We then proceed as in the proof of Theorem 10, with the difference that here m,n are half-integers. First, $(-1,0)$ is not a double in $E'_{22}(\mathbb{Q})$ because $-1-(-8m)\equiv 3 \pmod 8$ is not a square. Nor can $(-8m,0)$ be a double, since $-8m-(-1)\equiv 5 \pmod 8$. Similarly, $(-8n,0)$ cannot be a double. □

Theorem 14. *Consider the elliptic curve* $E_2: y^2+xy+y=x^3+2(2a-8b-1)x^2+ax+b$, *where* $a,b\in\mathbb{Z}$. *and recall that* $(-\frac14,-\frac38)$ *is a point of order* 2 *in* $E_2(\mathbb{Q})$.

(a) *If the equation* $t^2-(2a-8b-1)t+b+\frac14=0$ *in* t *has two distinct half-integer solutions* $m<n$, *then* E_2 *can be written as*

$$E_{22}: y^2+xy+y=x^3+2(m+n)x^2+\bigl(4mn+\tfrac12(m+n-1)\bigr)x+mn-\tfrac14$$

and $E_2(\mathbb{Q})$ *has a subgroup isomorphic to* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

(b) *Never does* $E_2(\mathbb{Q})$ *have a subgroup isomorphic to* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$.

(c) *Assuming the condition in (a) is met, the full torsion group is* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ *if and only if there exist integers* α, β *such that* $|\alpha|<\beta$, $\gamma:=-\alpha\beta/(\alpha+\beta)$ *is an integer*, $m=\frac{1}{8}(\alpha^2-\gamma^2+1)$, *and* $n=\frac{1}{8}(\beta^2-\gamma^2+1)$. *In this situation the points of order* 3 *have* x*-coordinate* $\frac{1}{4}(\gamma^2-1)$; *moreover* γ *is odd and* $\beta\equiv\alpha\equiv 2 \pmod 4$.

Proof. Parts (a) and (b) restate Theorem 13, apart from the easily checked equivalence between the conditions $a=4mn+\frac{1}{2}(m+n-1)$ and $b=mn-\frac{1}{4}$ in that theorem and m, n being the roots of the quadratic equation $t^2-(2a-8b-1)t+b+\frac{1}{4}=0$.

The proof of part (c) is verbatim the same as that of Theorem 12(d). (The condition $m,n\in\mathbb{Z}$ was not used in that proof except to show that α, β were divisible by 4. Here the condition $m,n\in\frac{1}{2}\mathbb{Z}\setminus\mathbb{Z}$ gives $\beta\equiv\alpha\equiv 2 \pmod 4$ instead.) □

5. Characterization of curves with torsion subgroup $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ in terms of Pythagorean triples

We now give a family of curves E_{11} whose torsion subgroup is isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$, and show that it is exhaustive.

Theorem 15. *Let* t *be a nonnegative integer and* (v,w,z) *a primitive Pythagorean triple with* v *even. For the integers*

$$s=\frac{v^2(4t+1)}{4},\ k=\frac{w^2(4t+1)-1}{4}\quad or\quad s=\frac{v^2(4t+3)}{4},\ k=-\frac{w^2(4t+3)+1}{4},$$

the conditions in part (c) of Theorem 12 are satisfied, so the elliptic curve E_{11} *written there has a torsion subgroup isomorphic to* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$.

Conversely, if E_{11} *in Theorem 12 has a torsion point of order* 8, *we are in the situation of part (c) of that theorem, with* s *and* k *arising from a primitive Pythagorean triple as above.*

Proof. Recall from the proof of Theorem 12(c) that the condition for the existence of torsion of order 8 is that there should be integers B, C satisfying either

$$B^2=s(1+4k+4s)\quad\text{and}\quad C^2=(1+4k)(1+4k+4s)\tag{5-1}$$

or

$$B^2=-s(1+4k-4s)\quad\text{and}\quad C^2=(1+4k)(1+4k-4s).\tag{5-2}$$

Substituting $s=\frac{1}{4}v^2(4t+1)$ and $k=\frac{1}{4}\big(w^2(4t+1)-1\big)$ on the left-hand sides of equalities (5-1) leads to

$$\tfrac{1}{4}v^2(4t+1)^2(v^2+w^2),\qquad w^2(4t+1)^2(v^2+w^2),$$

which are squares because v is even and $v^2+w^2=z^2$. Similarly, substituting $s=\frac{1}{4}v^2(4t+3)$ and $k=-\frac{1}{4}\big(w^2(4t+3)+1\big)$ in (5-2) also yields squares.

Conversely, suppose (5-1) is satisfied; our job is to find a Pythagorean triple as in the statement of Theorem 15. Combining the two equations (5-1) we get $4B^2+C^2=(1+4k+4s)^2$, so

$$(2B, C, 1+4k+4s)$$

is a Pythagorean triple. Let c be the gcd of the three members and (v, w, z) the corresponding primitive triple, so $2B=cv$, $C=cw$, $1+4k+4s=cz$. This last equation shows that c is odd, so v is even, so w is odd. Now note that

$$4s(1+4k+4s)=c^2v^2, \quad (1+4k)(1+4k+4s)=c^2w^2.$$

Since $cz=1+4k+4s$ divides both c^2v^2 and c^2w^2, and since v, w, z are relatively prime, we conclude that z divides c, that is, $c=zu$ for some odd integer u. Hence

$$4s=v^2u, \quad 1+4k=w^2u. \tag{5-3}$$

This last equation gives $u\equiv 1 \pmod 4$ since $w^2\equiv 1 \pmod 4$. Thus we can write $u=4t+1$ for some integer $t\geq 0$, and from (5-3) we get

$$s=\frac{v^2(4t+1)}{4} \quad \text{and} \quad k=\frac{w^2(4t+1)-1}{4},$$

as needed.

A wholly analogous reasoning shows that when (5-2) is satisfied, instead of (5-1), there is a Pythagorean triple (v, w, z) (with v even) and an integer $t\geq 0$ such that

$$s=\frac{v^2(4t+3)}{4} \quad \text{and} \quad k=-\frac{w^2(4t+3)+1}{4}. \qquad \square$$

Remark 16. Every elliptic curve over $\mathbb{Q}$ with torsion group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ is isomorphic to one of those in Theorem 15. Indeed, it is known (see [Campbell and Goins 2004, Theorem 6.2], for example) that every such curve has an equation of the form

$$y^2=x(x+u^2)(x+u^{-2}), \quad \text{for } u=\frac{T^2-1}{2T} \text{ with } T\in\mathbb{Q}\setminus\{0, 1, -1\}.$$

It's easy to see that there is a primitive Pythagorean triple (v, w, z) with $v/w=u$, and by interchanging v and w if necessary we can ensure that v is even. To go from the form

$$y^2=x\Big(x+\frac{w^2}{v^2}\Big)\Big(x+\frac{v^2}{w^2}\Big)$$

to the desired form of E_{11}, we apply affine coordinate changes with rational coefficients: the scaling $(x, y)\mapsto(4xv^{-2}w^{-2}, 8yv^{-3}w^{-3})$, followed by the change of parameters $s = \frac{1}{4}v^2$ and $k = \frac{1}{4}(w^2 - 1)$ (case $t = 0$ in the first set of substitution in Theorem 15), gives

$$y^2 = x\big(x + (2s)^2\big)\big(x + (2k + \tfrac{1}{2})^2\big);$$

further inserting the values $m = -k - 2k^2$ and $n = -k - 2k^2 + 2s^2$ and applying the coordinate change $x \mapsto x + 2m$ followed by $y \mapsto y + x/2$ leads to the canonical form of E_{11}.

References

[Campbell and Goins 2004] G. Campbell and E. H. Goins, "Heron triangles, Diophantine problems and elliptic curves", preprint, 2004, Available at http://www.swarthmore.edu/NatSci/gcampbe1/papers/heron-Campbell-Goins.pdf.

[Knapp 1992] A. W. Knapp, "Elliptic curves", 1992. MR 93j:11032 Zbl 0804.14013

[Mazur 1977] B. Mazur, "Modular curves and the Eisenstein ideal", *Inst. Hautes Études Sci. Publ. Math.* 47 (1977), 33–186. MR 80c:14015 Zbl 0394.14008

Received October 26, 2007. Revised September 2, 2008.

SUMI JEONG
DEPARTMENT OF MATHEMATICS AND INSTITUTE OF PURE AND APPLIED MATHEMATICS
CHONBUK NATIONAL UNIVERSITY
JEONJU, JEONBUK 561-756
REPUBLIC OF KOREA
sumi@chonbuk.ac.kr

HWASIN PARK
DEPARTMENT OF MATHEMATICS AND INSTITUTE OF PURE AND APPLIED MATHEMATICS
CHONBUK NATIONAL UNIVERSITY
JEONJU, JEONBUK 561-756
REPUBLIC OF KOREA
park@chonbuk.ac.kr