## 2.5 Exercise Sheet 5

### 2.5.A Numerical and Exploration

**Exercise 2.5.1.** Let $E/\mathbb{Q}$ be the elliptic curve $E : y^2 = x^3 + x$.

(a) For each $n = 1, 2, 3, 4$, explicitly write down all the elements of, and determine the groups structures of, $E[n](\mathbb{Q})$ and $E[n](\overline{\mathbb{Q}})$. How many points of each order do we have in each of these groups? Does 1.12.27 hold?

(b) (For those who have seen some Galois theory.) For each $n = 1, 2, 3, 4$, let $K_n/\mathbb{Q}$ denote the number field generated by the $x$- and $y$-coordinates of all the points $P \in E[n](\overline{\mathbb{Q}})$. Determine the degree $[K_n : \mathbb{Q}]$. Is $K_n/\mathbb{Q}$ Galois? If so, what is $\mathrm{Gal}(K_n/\mathbb{Q})$? For which $n$ does $K_n$ contain $\mathbb{Q}[i]$? When it does, what can you say about $\mathrm{Gal}(K_n/\mathbb{Q}[i])$? When it doesn't, what can you say about $\mathrm{Gal}(K_n \cdot \mathbb{Q}[i]/\mathbb{Q}[i])$? (Hint: It might be helpful to get Sage to factor a sextic polynomial.)

(c) Repeat the same as in (a) and (b) for the curve $E : y^2 = x^3 + 1$. Note that you may wish to replace $\mathbb{Q}[i]$ in (b) by some other imaginary quadratic number field (which one?). (Hint: The cases $n = 1, 2, 3$ can be done easily by hand. You may use Sage for $n = 4$.)

(d) (**) Make and prove conjectures generalizing your results from (a), (b), and (c). (Hint: Can you generalize these results to curves of the form $y^2 = x^3 + bx$? To curves of the form $y^2 = x^3 + c$? To curves with complex multiplication?)

**Exercise 2.5.2.**

(a) Does every finitely generated abelian group $A$ admit a height function, i.e., a function $h : A \to [0, \infty)$ satisfying conditions (a), (b), (c) of 1.15.11?

(b) Is the map $\mathbb{Q} \to [0, \infty)$ given by $q \mapsto h(q)$ a height function on the additive group $\mathbb{Q}$? Is the same map a height function on the multiplicative group $\mathbb{Q}^\times$?

(c) Determine, for each of the following fields $K$,
   (i) if $K/2K$ is finite,
   (ii) if $K$ admits a height function,
   (iii) if $K^\times/(K^\times)^2$ is finite, and
   (iv) if $K^\times$ admits a height function.
   Consider $K = \mathbb{Q}, \mathbb{F}_q, \mathbb{R}, \mathbb{C}, \mathbb{F}_2(t)$. If you know about the $p$-adic numbers, also consider $K = \mathbb{Q}_p$.

**Exercise 2.5.3.** Let $E/\mathbb{Q}$ be the elliptic curve $E : y^2 = x^3 - 7x + 10$. Consider the points $P = (1, 2)$ and $Q := (3, 4)$ on $E$.

(a) Use Sage to compute $mP + nQ$ for all $m, n \in \mathbb{Z}$ with $-10 \le m, n \le 10$, and check if $mP + nQ = \mathscr{O}$ for any of these values of $m$ and $n$.

(b) Use Sage to compute the Néron-Tate canonical heights of $P, Q$, and $P+Q$. (Hint: You can get Sage to return the canonical height of a point `P` on an elliptic curve over $\mathbb{Q}$ by asking for `P.height()`.)

(c) Are $P$ and $Q$ $\mathbb{Z}$-linearly dependent in the group law on $E$? In other words, are there integers $m, n \in \mathbb{Z}$, not both zero, such that $mP + nQ = \mathscr{O}$? (Hint: Use (b) to make a suitable $2\times2$ matrix, and then compute its determinant. You can either trust Sage's floating-point arithmetic (highly recommended!), or very tediously verify it yourself to sufficient accuracy.)

(d) Repeat the same as in (a), (b), and (c) for a few other curves $E/\mathbb{Q}$ and pairs of points $P, Q \in E(\mathbb{Q})$ of your choosing (obtained either by just experimentation in Sage, or from the LMFDB). Formulate a general criterion in terms of the Néron-Tate height pairing to determine whether or not a set of points $P_1, \ldots, P_n \in E(\mathbb{Q})$ is $\mathbb{Z}$-linearly dependent.

**Exercise 2.5.4.** Using the method explained in class (descent via 2-isogeny), compute the ranks of the following elliptic curves $E/\mathbb{Q}$ by hand, and then check your answer with Sage. Further, in each case, determine a full set of coset representatives for $E(\mathbb{Q})/2E(\mathbb{Q})$.

(a) $y^2 = x^3 + 7x$
(b) $y^2 = x^3 - 12x^2 + 20x$
(c) $y^2 = x^3 - 3x^2 + 10x$
(d) $y^2 = x^3 - 377x$

(Hint: This is NOT a random list–the numbers are specifically chosen so that the computations are easily doable by hand! Remark: To get an idea of the sort of thing Sage is doing when you call `rank()`, you can either do `E.rank?` or `print(E.mwrank())` for a given curve `E`.)

### 2.5.B PODASIPs

Prove or disprove and salvage if possible the following statements.

**Exercise 2.5.5.** (Adapted from [2, Exercise 3.2]) Let $E/\mathbb{Q}$ be an elliptic curve in short Weierstrass form $E : y^2 = x^3 + ax^2 + bx + c$ with $a, b, c \in \mathbb{Z}$. There is a constant $C_5 \in \mathbb{R}_{\geq 0}$ depending only on $a, b, c$ such that for all $P, Q \in E(\mathbb{Q})$, we have

$$|h(P+Q) + h(P-Q) - 2(h(P) + h(Q))| \leq C_5.$$

(Hint: Express $x(P+Q)+x(P-Q)$ and $x(P+Q)\cdot x(P-Q)$ in terms of $x(P)$ and $x(Q)$ alone. Then try something similar to what we did in class to get one direction of the inequality. To get the other direction, use the direction already proven along with the inequality $h(2P) \geq 4h(P) - C_3$ from class.)

**Exercise 2.5.6.** Let $E_1, E_2$ be isomorphic elliptic curves over $\mathbb{Q}$ in Weierstrass form, and let $\varphi : E_1 \to E_2$ be an isomorphism, i.e., an admissible change of coordinates. Then for any point $P \in E_1(\mathbb{Q})$, we have that

$$\hat{h}_1(P) := \lim_{N\to\infty} \frac{1}{4^N} h(x(2^N P)) = \lim_{N\to\infty} \frac{1}{4^N} h(x(\varphi(2^N P))) =: \hat{h}_2(P).$$

In particular, the Néron-Tate canonical height on an elliptic curve $E$ is independent of the choice of Weierstrass equation for $E$, and only depends on its isomorphism type over $\mathbb{Q}$.

**Exercise 2.5.7.** Let $E/\mathbb{Q}$ be an elliptic curve in Weierstrass form, and let $\hat{h} : E(\mathbb{Q}) \to [0, \infty)$ be the Néron-Tate canonical height on $E$. For any $P \in E(\mathbb{Q})$ and $T \in \operatorname{Tors} E(\mathbb{Q})$, we have that $\hat{h}(P+T) = \hat{h}(P)$. In other words, $\hat{h}$ is insensitive to the addition of torsion points on $E(\mathbb{Q})$.

**Exercise 2.5.8.** Let $E/\mathbb{Q}$ be an elliptic curve.

(a) For all $P \in E(\mathbb{Q})$, we have

$$\hat{h}(P) = \lim_{m\to\infty} \frac{1}{m^2} h(mP).$$

(b) For all $P \in E(\mathbb{Q})$, we have

$$\lim_{N\to\infty} \frac{1}{4^N} h(y(2^N P)) = \frac{3}{2} \cdot \hat{h}(P).$$

More generally, for any $f \in \mathbb{Q}(E)$, there is a constant $d \in \mathbb{Q}$ depending only on $f$ such that for all $P \in E(\mathbb{Q})$,

$$\lim_{N\to\infty} \frac{1}{4^N} h(f(2^N P)) = \frac{d}{2} \cdot \hat{h}(P).$$

(c) $(*)$ Suppose $p \in [0, \infty]$. Define the $\ell_p$ height $H_p$ (resp. *logarithmic $\ell_p$ height* $h_p$) of a rational number $q = u/v$ in lowest terms to be

$$H_p(q) := \left(\frac{|u|^p + |v|^p}{2}\right)^{1/p} \text{ (resp. } h_p(q) := \log H_p(q)).$$

(What does this mean for $p \in \{0, \infty\}$?) For any $p \in [0, \infty]$ and any $P \in E(\mathbb{Q})$, we have

$$\lim_{N\to\infty} \frac{1}{4^N} h_p((2^N P)) = \hat{h}(P).$$

In other words, we could have equally well chosen $h_p$ as our definition of the naive height, and we would have obtained the same definition of the canonical height.

**Exercise 2.5.9.** Let $A$ be an abelian group and $R$ a ring (the two cases we'll be most interested in are $R = \mathbb{Z}$ and $R = \mathbb{R}$). A map $q : A \to R$ is said to be an *$R$-valued quadratic form* iff the following two conditions hold:

(a) For all $a \in A$ and all $n \in \mathbb{Z}$, we have $q(na) = n^2 q(a)$.
(b) The map $\langle \cdot, \cdot \rangle : A \times A \to R$ defined by

$$\langle a, b \rangle := q(a+b) - q(a) - q(b)$$

for $a, b \in A$ is $\mathbb{Z}$-bilinear, i.e., satisfies for all $a_1, a_2, b \in A$ that

$$\langle a_1 + a_2, b\rangle = \langle a_1, b\rangle + \langle a_2, b\rangle,$$

and similarly for the other side.

This is the abelian group analog of an inner product on vector spaces. PODASIP: A map $q : A \to R$ of sets is a(n) ($R$-valued) quadratic form iff the parallelogram law holds, i.e., for all $a, b \in A$, we have

$$q(a + b) + q(a - b) = 2q(a) + 2q(b).$$

**Exercise 2.5.10.** (For those who have taken a course on linear algebra.) Let $r \in \mathbb{Z}_{\geq 0}$, let $A := \mathbb{Z}^{\oplus r}$, and let $V := \mathbb{R} \otimes_{\mathbb{Z}} A \cong \mathbb{R}^r$, so that $A \subset V$ as a full-rank lattice.

(a) Suppose that $q : A \to \mathbb{R}$ is a quadratic form with the following two properties.
   (i) For $a \in A$, we have that $q(a) = 0$ iff $a = 0$.
   (ii) For every constant $C_1 \in \mathbb{R}_{\geq 1}$, the set $\{a \in A : q(a) \leq C_1\}$ is finite.
   Then $q$ extends to a positive definite quadratic form on $V$. (Hint: Pick a suitable basis for $V$ in which the extended $q : V \to \mathbb{R}$ is diagonal (what does that mean?). If $q$ is *not* positive definite, then a clever application of Minkowski's Theorem finds a lattice point (i.e., an $a \in A$) with $q$-size less than $\inf_{a \in A \smallsetminus \{0\}} q(a)$.)

(b) (**) Is the condition (ii) necessary in (a) above? Is it necessary if we allow $A$ to have infinite rank? Can you make sense of [8, Remark VIII.9.4]?

**Exercise 2.5.11.** A sequence of homomorphisms of abelian groups

$$\cdots \xrightarrow{\partial^{i-1}} A^i \xrightarrow{\partial^i} A^{i+1} \xrightarrow{\partial^{i+1}} \cdots$$

is said to be a *complex* if $\partial^2 = 0$ (i.e., for all $i$ we have $\partial^{i+1}\partial^i = 0 : A^i \to A^{i+2}$). It is said to be an *exact complex* or an *exact sequence* iff $\ker \partial^{i+1} = \operatorname{im} \partial^i$ for all $i$.

(a) A sequence of the form $0 \to A \xrightarrow{f} B$ is exact iff $f$ is injective. A sequence of the form $B \xrightarrow{g} C \to 0$ is exact iff $g$ is surjective. A sequence of the form $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is exact iff $f$ is injective, $g$ is surjective, and $f$ takes $A$ isomorphically to $\ker g$, i.e., iff $f$ is injective and $B/f(A) \xrightarrow{\sim} C$.

(b) If $0 \to A \to B \to C \to 0$ is an exact sequence of abelian groups, then if two of $A, B, C$ are finite, then so is the third. If this holds, then the sizes of $A, B$, and $C$ are related by $\#B = \#A \cdot \#C$. (Hint: The First Isomorphism Theorem.)

(c) Generalize (b) to exact sequences of any (finite) length. Specifically, if $n \in \mathbb{Z}_{\geq 0}$ and

$$0 \to A^0 \xrightarrow{\partial^0} A^1 \xrightarrow{\partial^1} \cdots \to A^n \to 0$$

is an exact sequence of finite abelian groups, and all but one of the $A^i$ are finite, then all are finite. In this case, the sizes of the $A^i$ are related by

$$\prod_{i=0}^{n} (\#A^i)^{(-1)^i} = 1.$$

(Hint: Break the "long exact sequence" into several "short exact sequences" of the form $0 \to \ker \partial^i \to A^i \to \ker \partial^{i+1} \to 0$, and then apply (a).)

(d) If $A \xrightarrow{f} B \xrightarrow{g} C$ is a sequence of homomorphisms of abelian groups, then we have an exact sequence of the form

$$0 \to \ker(f) \to \ker(gf) \xrightarrow{f} \ker(g) \to \operatorname{coker}(f) \xrightarrow{g} \operatorname{coker}(gf) \to \operatorname{coker}(g) \to 0.$$

In particular, if $\operatorname{coker}(f)$, and $\operatorname{coker}(g)$ are finite, then so is $\operatorname{coker}(gf)$. If further $\ker(f), \ker(gf)$ and $\ker(g)$ are also finite, then the sizes of these groups are related by

$$\#\ker(f) \cdot \#\ker(g) \cdot \#\operatorname{coker}(gf) = \#\ker(gf) \cdot \#\operatorname{coker}(f) \cdot \#\operatorname{coker}(g).$$

**Exercise 2.5.12.** If $A$ is a finitely generated abelian group, then for any $n \in \mathbb{Z}_{\geq 1}$, we have that

$$\#A[n] = \#A/nA.$$

**Exercise 2.5.13.** Let $K$ be a field of characteristic other than 3, and suppose further that $K$ contains a primitive cube root of unity $\omega$. (For example we could take $K = \mathbb{C}$ or $K = \mathbb{F}_p$ for a prime $p$ such that $p \equiv 1 \pmod 3$.) Let $c \in K^\times$ and let $E/K$ be the elliptic curve $E : y^2 = x^3 + c$. Let $[\omega] : E \to E$ be the automorphism given by $[\omega](x, y) := (\omega x, y)$. Then $[\omega]^2 + [\omega] + 1 = 0$ as maps from $E$ to $E$, i.e., for all extensions $L/K$ and $P \in E(L)$ we have that $[\omega]([\omega]P) + [\omega]P + P = \mathscr{O}$ in $E(L)$.

**Exercise 2.5.14.** Let $E/\mathbb{F}_3$ be the elliptic curve $y^2 = x^3 + x^2 - x$. The formula

$$(x, y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(x^2+1)}{x^2}\right)$$

defines a self-map $\phi : E \to E$. There are unique $t, n \in \mathbb{Z}_{\geq 1}$ such that $\phi^2 - [t] \circ \phi + [n] = 0$ as maps from $E$ to $E$, i.e., such that for all extensions $L/\mathbb{F}_3$ and $P \in E(L)$ we have that $\phi(\phi(P)) - \phi(tP) + nP = \mathscr{O}$ in the group $E(L)$. (This is an example of an endoisogeny of degree 2.)

**Exercise 2.5.15.** (For those who have taken a course on number fields.) Let $K$ be a number field with ring of integers $\mathscr{O}_K$, and let $S$ be a finite set of primes (or equivalently non-archimedean places) of $\mathscr{O}_K$. For each integer $n \in \mathbb{Z}_{\geq 1}$, define the subgroup $K(S, n) \subset K^\times/(K^\times)^n$ by

$$K(S, n) := \{[a] \in K^\times/(K^\times)^n : \text{ for all } \mathfrak{p} \notin S \text{ we have } v_\mathfrak{p}(a) \equiv 0 \pmod n\}.$$

(a) For instance, if $K = \mathbb{Q}$, then $S$ is a finite set of prime numbers, and $\mathbb{Q}(S, n) \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^n$ is the subgroup generated by $\pm 1$ and the images of the elements of $S$. In this case, $\#\mathbb{Q}(S, n) \leq 2 \cdot n^{\#S}$. (You may wish to improve this estimate depending on the parity of $n$.)

(b) In general, for any number field $K$ and $S$ and $n$, the group $K(S, n)$ is finite. Can you give an upper bound on the size of $\#K(S, n)$? (Hint: Describe a diagram of the form

$$\begin{array}{ccccccc} & & 0 & & & & \\ & & \downarrow & & & & \\ & & \mathscr{O}_K^\times/(\mathscr{O}_K^\times)^n & & & & \\ & & \downarrow & & & & \\ 0 & \longrightarrow & K(\emptyset, n) & \longrightarrow & K(S, n) & \longrightarrow & (\mathbb{Z}/n)^{\#S} \\ & & \downarrow & & & & \\ & & \mathrm{Cl}(K), & & & & \end{array}$$

where the row and column are exact, and use two fundamental finiteness results from the theory of number fields. Bonus question: what is the image of $K(\emptyset, n) \to \mathrm{Cl}(K)$?)

**Exercise 2.5.16** (A 3-Isogeny). (Adapted from [1, Exercise 14.5].) (**) Let $K = \mathbb{Q}$ (for simplicity). Let $c \in K^\times$, and consider the elliptic curve $E : y^2 = x^3 + c$. We will show that $E(K)/3E(K)$ is finite.

For simplicity, suppose also that $c$ is not a square in $K$, and let $\gamma \in \overline{K}$ be a square root of $c$, i.e., so that $\gamma^2 = c$. Finally, let $L := K[\gamma]$, so that $L$ is a quadratic extension of $K$.

(a) We have $T^\pm = (0, \pm\gamma) \in E[3](L)$, and that $2T^+ = T^-$ and $2T^- = T^+$.

(b) Find a formula for the operation $\tau_{T^\pm} : E \to E$ given by $P \mapsto P + T^\pm$. In other words, given $P = (x, y) \in E(L)$, express the $x$- and $y$-coordinates of $P + T^\pm$ in terms of those of $P$ and $\gamma$.

(c) Let $P = (x, y) \in E(K)$. Express the following quantities as rational functions in $x$ and $y$:

$$\xi := x(P) + x(P + T^+) + x(P + T^-) \text{ and } \eta := y(P) + y(P + T^+) + y(P + T^-).$$

Simplify until $\xi$ and $\eta \cdot y^{-1}$ are functions of $x$ alone.

(d) The rational functions $\xi$ and $\eta$ as in (c) satisfy an equation of the form $\eta^2 = \xi^3 + c'$ for some $c' \in K^\times$. Express $c'$ in terms of $c$. If $E' : y^2 = x^3 + c'$, then $(x, y) \mapsto (\xi, \eta)$ defines a map $\phi : E \to E'$.

(e) As done in class, define a map $\phi' : E' \to E$ by essentially the same formula as for $\phi$, except for $c'$ replacing $c$, and some factors of 3 (which you should figure out). In this case, $\phi' \circ \phi : E \to E$ is the triplication map $[3] : E \to E$, and the same is true of the map $\phi \circ \phi' : E' \to E'$. (Hint: You may use Sage to speed up computations if this is helpful. See also 2.2.10(c).)

(f) The induced maps $\phi : E(K) \to E'(K)$ and $\phi' : E(K) \to E'(K)$ are group homomorphisms. (Hint: By symmetry, it suffices to show the result for $\phi$. Use 1.15.5 and 1.12.17 to reduce to showing that if $P_1, P_2, P_3 \in E(K)$ are collinear, then so are $\phi(P_1), \phi(P_2)$ and $\phi(P_3)$. Now suppose that $P_1, P_2, P_3$ lie on the line $y = \lambda x + \nu$. Show that $\phi(P_1), \phi(P_2)$, and $\phi(P_3)$ lie on the line $y = \lambda' x + \nu'$, where

$$(\lambda', \nu') = \left( \frac{\lambda(\nu^2 + 3c)}{\nu^2 - c}, \frac{\nu^3 - 4c\lambda^3 - 9c\nu}{\nu^2 - c} \right).$$

In proving this, you may need to make use of the identity

$$(\lambda x + \nu)(x^3 - 8c) - \lambda' x(x^3 + 4c) - \nu' x^3 + \left( \frac{4c(\lambda x - 2\nu)}{\nu^2 - c} \right) (x^3 - (\lambda x + \nu)^2 + c) = 0,$$

which you can check on a computer algebra software like Sage. Finally, you will have to deal with some edge cases separately. )

(g) Suppose that $P = (x, y) \in E(K)$ has the property that $y + \gamma$ is a cube in $L$. Then there is a $P' \in E'(K)$ such that $P = \phi'(P')$. (Hint: Write $y + \gamma = (u + v\gamma)^3$, expand, and compare coefficients. Then use the formula for $\phi'$ to figure out what $P'$ should be in terms of $u$ and $v$.)

(h) The map $\alpha : E(K) \to L^\times/(L^\times)^3$ given by $(x, y) \mapsto [y + \gamma]$ is a group homomorphism with kernel precisely $\phi'(E'(K))$. In particular, $\alpha$ induces an injective homomorphism $E(K)/\phi'(E'(K)) \hookrightarrow L^\times/(L^\times)^3$.

(i) The image $\operatorname{Im}\alpha \subset L^\times/(L^\times)^3$ is finite. In particular, $E(K)/3E(K)$ is finite. (Hint: $\operatorname{Im}\alpha \subset L(S, 3)$ for a suitably chosen $S$.)

(j) Try to figure out what to do when $c$ *is* a square in $K$. Which parts of the above argument still work, and which need to be modified? Can they be modified? (Hint: Let $L$ still be $K[x]/(x^2 - c)$, even though this is no longer a field.)

(k) To what extent was the above analysis dependent on the fact that $K = \mathbb{Q}$? Over what other fields $K$ do the above results still hold?

**Exercise 2.5.17.** (For those who have taken a course on number fields.) $(*)$ Let us finish the proof started in class of Fermat's Last Theorem for $n = 3$. Recall that in 1.2.B, we reduced the problem to showing that if $E/\mathbb{Q}$ is the elliptic curve $E : y^2 = x^3 - 432$, then $E(\mathbb{Q}) = \{\mathscr{O}, (12, \pm 36)\}$. As in class, let $L$ be the cubic number field $L := \mathbb{Q}[\gamma]$ where $\gamma^3 = 2$, and let $\beta := 6\gamma$, so that $x^3 - 432 = (x - \beta)(x^2 + \beta x + \beta^2) \in L[x]$. Let $\alpha : E(\mathbb{Q}) \to L^\times/(L^\times)^2$ be the morphism defined in class, so that $\ker\alpha = 2E(\mathbb{Q})$.

(a) We have $\operatorname{Tors} E(\mathbb{Q}) = \{\mathscr{O}, (12, \pm 36)\}$. In particular, it suffices to show that $\operatorname{Im}\alpha = \{1\}$.

(b) We have that $\mathscr{O}_L = \mathbb{Z}[\gamma]$, and this is a UFD. The only rational primes that ramify in $L$ are 2 and 3, and both are totally ramified: $(2) = (\gamma)^3$ and $(3) = (\gamma + 1)^3$. Further, $L$ has fundamental unit $\gamma - 1$, so that $\mathscr{O}_L^\times = \{\pm(\gamma - 1)^{\mathbb{Z}}\}$. (Hint: See Exercises 2.41, 5.19, and 5.36 of [18].)

(c) In the notation from class, we have that $q(x) = x^2 + \beta x + \beta^2$, so that $q(\beta) = 108\gamma^2$. This factors in $\mathscr{O}_L$ as $(q(\beta)) = (\gamma)^8(\gamma + 1)^9$. In particular, if $S = \{(\gamma), (\gamma + 1)\}$, then $\operatorname{Im}\alpha \subset L(S, 2)$.

(d) By 2.5.15, the subgroup $L(S, 2) \subset L^\times/(L^\times)^2$ has size exactly 16. Explicitly, $\mathscr{O}_L^\times/(\mathscr{O}_L^\times)^2 \cong (\mathbb{Z}/2)^{\oplus 2}$ with elements represented by $\pm 1, \pm(\gamma - 1)$, and so $L(S, 2)$ has exactly 16 elements, represented by $\pm 1, \pm(\gamma - 1), \pm\gamma, \pm(\gamma^2 - \gamma), \pm(\gamma + 1), \pm(\gamma^2 - 1), \pm(\gamma^2 + \gamma), \pm(\gamma^3 - \gamma)$. (This shows already that $\operatorname{rank} E \leq 4$.)

(e) If $(x, y) \in E(\mathbb{Q}) \smallsetminus \{\mathscr{O}\}$, then under the real embedding $L \hookrightarrow \mathbb{R}$, we have $x - 6\gamma > 0$. In particular, no element with negative sign in the list in (d) is an element of $\operatorname{Im}\alpha$, i.e., $\operatorname{Im}\alpha \subset \{1, \gamma, \gamma \pm 1, \gamma^2 \pm \gamma, \gamma^2 - 1, 2 - \gamma\}$.

(f) For any $(x, y) \in E(\mathbb{Q}) \smallsetminus \{\mathscr{O}\}$, we have that $v_\gamma(x - \beta) \equiv 0 \pmod 2$. In particular, $\operatorname{Im}\alpha \subset \{1, \gamma \pm 1, \gamma^2 - 1\}$. (Hint: Write $(x, y) = (m/e^2, n/e^3)$ as in 1.14.8, so that

$$n^2 = (m - 6e^2\gamma)(m^2 + 6me^2\gamma + 36e^4\gamma^2).$$

If $v_\gamma(x - \beta) \equiv 1 \pmod 2$, then $\gamma \mid m$ and so $m$ and $n$ are even and $e$ is odd. Write $m = 2m_1$ and $n = 2n_1$ for $m_1, n_1 \in \mathbb{Z}$; then in fact $2 \mid n_1$ and so $2 \mid m_1$. In particular, $v_\gamma(m_1 - 3e^2\gamma) = 1$, so that $v_\gamma(m - 6e^2\gamma) = 4$, a contradiction.)

(g) For any $(x, y) \in E(\mathbb{Q}) \smallsetminus \{\mathscr{O}\}$, we have that $v_{\gamma+1}(x - \beta) \equiv 0 \pmod 2$. In particular, $\operatorname{Im}\alpha \subset \{1, \gamma - 1\}$. (Hint: If $\gamma + 1 \mid m$, then $m$ and $n$ are divisible by 3 and $e$ is not. Write $m = 3m_1$ and $n = 3n_1$. Then $\gamma + 1$ divides either $m_1^2 - 2e^2\gamma$ or $m_1^2 + 2m_1e^2\gamma + 4e^4\gamma^2$. In the former case, $3 \mid m_1 + 2e^2$ and $v_{\gamma+1}(m_1 - 2e^2\gamma) = 1$, so that $v_{\gamma+1}(m - 6e^2\gamma) = 4$, a contradiction. In the latter case (and when *not* in the former), we get a contradiction to the fact that 3 totally ramifies in $L$.)

(h) It only remains to exclude the possibility that $\gamma - 1 \in \operatorname{Im}\alpha$, so suppose this happens. Then $x - 6\gamma = (\gamma - 1)(u\gamma^2 + v\gamma + w)^2$ for some $u, v, w \in \mathbb{Q}$, not all zero. Expanding, this gives us the system of equations

$$\begin{cases} x & = -4uv + 2v^2 + 4uw - w^2, \\ -6 & = -2u^2 + 4uv - 2vw + w^2, \text{ and} \\ 0 & = 2u^2 - v^2 - 2uw + 2vw. \end{cases}$$

The last conic $\mathbb{V}(2u^2 - v^2 - 2uw + 2vw) \subset \mathbb{P}^2_{\mathbb{Q}}$ admits the rational parametrization $[u : v : w] = [t(t+2s) : 2t(t+s) : t^2 - 2s^2]$. Plugging this into the second equation gives us a nontrivial rational point on

$$-6r^2 = 4s^4 + 8s^3t + 12s^2t^2 + 12st^3 + 3t^4,$$

but such a point does not exist. (Hint: Find a local obstruction to the existence of a rational point on this hyperelliptic curve. This example explains why the theory of binary quartics shows up in the investigation of rational points on elliptic curves.)

This finishes the proof of Fermat's Last Theorem for $n = 3$.