RANKS OF ELLIPTIC CURVES VIA CLASS GROUPS OF NUMBER FIELDS

Abstract. Poincaré conjectured, and Mordell proved, that the collection of rational points of an elliptic curve defined over the rational numbers is a finitely generated abelian group. Weil generalized this to elliptic curves defined over number fields. In many cases, the torsion subgroup of an elliptic curve, even over a number field, is easy to compute. On the other hand, the rank is not.

In this talk, we discuss ways to compute the rank of an elliptic curve by discussing two cases in detail. First, we review how to compute the rank assuming there is a rational point of order two by introducing binary quartic forms as covering spaces. Second, we discuss state-of-the art methods to compute the rank assuming there is no rational point of order two by introducing the class group of certain cubic extensions. This is joint work with Jamie Weigandt.

Preliminaries

Number Fields. Let K be a number field, that is, a finite extension of $\mathbb{Q}$. We will denote $\mathcal{O}_K$ as the integral closure of $\mathbb{Z}$ in K; this is the collection of algebraic integers in K. In practice, we will choose $K = \mathbb{Q}$ so that $\mathcal{O}_K = \mathbb{Z}$.

Let S be a finite set of primes of K containing the infinite places of K. For each place $\mathfrak{p} \notin S$ of K, we have valuation $\mathrm{ord}_{\mathfrak{p}} : K \hookrightarrow K_{\mathfrak{p}} \to \mathbb{Z} \cup \{\infty\}$. If L is a finite extension of K which is unramified outside of S, then there is a finite place $\mathfrak{P}$ of L lying over $\mathfrak{p}$, and we can uniquely extend $\mathrm{ord}_{\mathfrak{p}}$ to a valuation $\mathrm{ord}_{\mathfrak{P}} : L \hookrightarrow L_{\mathfrak{P}} \to \mathbb{Z} \cup \{\infty\}$. Define the S-integers of L as the ring

$$\mathcal{O}_{L,S} = \left\{ x \in L \;\middle|\; \mathrm{ord}_{\mathfrak{P}}(x) \geq 0 \text{ for all } \mathfrak{P} \text{ lying over } \mathfrak{p} \notin S \right\}.$$

Later, we will focus on the multiplicative group $U_S(L) = \mathcal{O}_{L,S}^{\times}$ as the S-units of L.

Elliptic Curves. Consider now a cubic curve in the form

$$E: \quad y^2 + a_1\, x\, y + a_3\, y = x^3 + a_2\, x^2 + a_4\, x + a_6$$

for some algebraic integers $a_i \in \mathcal{O}_K$. It is standard to introduce the coefficients

$$b_2 = a_1^2 + 4\, a_2 \qquad c_4 = b_2^2 - 24\, b_4$$

$$b_4 = 2\, a_4 + a_1\, a_3 \qquad c_6 = -b_2^3 + 36\, b_2\, b_4 - 216\, b_6$$

$$b_6 = a_3^2 + 4\, a_6 \qquad \Delta = -b_2^2\, b_8 - 8\, b_4^3 - 27\, b_6^2 + 9\, b_2\, b_4\, b_6$$

$$b_8 = a_1^2\, a_6 + 4\, a_2\, a_6 - a_1\, a_3\, a_4 + a_2\, a_3^2 - a_4^2$$

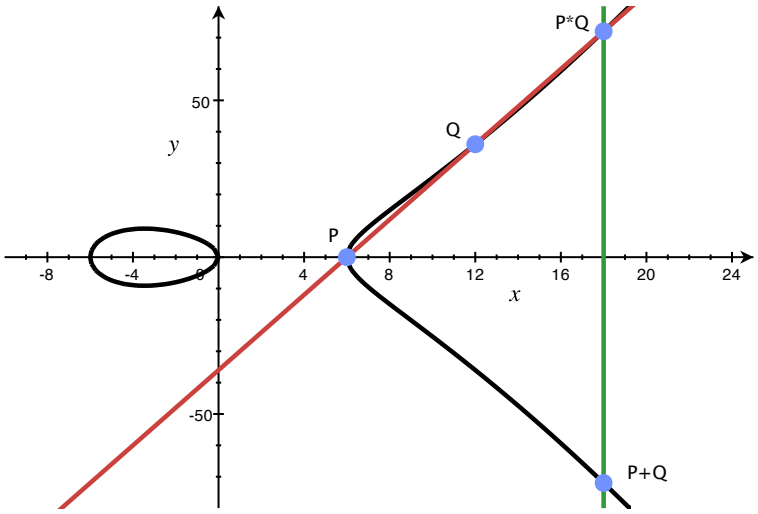
We will assume that $\Delta \neq 0$, that is, that E is an elliptic curve. In practice, we will choose $L = K[x]/(\psi_2(x))$ in terms of the 2-division polynomial $\psi_2(x) = 4\, x^3 + b_2\, x^2 + 2\, b_4\, x + b_6$; and S as the set of places of K containing all of the archimedean places, all places dividing 2, and all places which divide the discriminant Δ.

Mordell-Weil Group. The collection of K-rational points on E is the Zariski closure of the collection of K-rational affine points:

$$E(K) = \left\{ (x_1 : x_2 : x_0) \in \mathbb{P}^2(K) \,\middle|\, \begin{array}{r} x_2^2\,x_0 + a_1\,x_1\,x_2\,x_0 + a_3\,x_2\,x_0^2 \\ = x_1^3 + a_2\,x_1^2\,x_0 + a_4\,x_1\,x_0^2 + a_6\,x_0^3 \end{array} \right\}$$

$$= \left\{ (x, y) \in \mathbb{A}^2(K) \,\middle|\, y^2 + a_1\,x\,y + a_3\,y = x^3 + a_2\,x^2 + a_4\,x + a_6 \right\} \cup \{\mathcal{O}\}$$

in terms of the "point at infinity" $\mathcal{O} = (0 : 1 : 0)$. It is easy – but nontrivial! – to see that $E(K)$ is an abelian group via the Chord Tangent construction: denoting $P * Q$ as the third point of intersection of the cubic curve with a line through P and Q, define $P \oplus Q = \big(P * Q\big) * \mathcal{O}$.



In 1908, Jules Henri Poincaré conjectured that $E(K)$ is a finitely abelian group when $K = \mathbb{Q}$; this was shown by Louis Joel Mordell in 1922. In 1928, André Weil generalized this for any number field K. The Fundamental Theorem of Finitely Generated Abelian Groups asserts that

$$E(K) \simeq E(K)_{\text{tors}} \times \mathbb{Z}^r$$

for some finite group $E(K)_{\text{tors}}$ (called the torsion subgroup of the elliptic curve) and some nonnegative integer r (called the rank of the elliptic curve). This set is often called the Mordell-Weil group of the elliptic curve E.

Torsion Subgroup. The torsion subgroup $E(K)_{\text{tors}}$ is somewhat easy to compute. In 1949, John William Scott Cassels showed that if $(x : y : 1) \in E(K)$ has exact order m, that is, $[m]P = \mathcal{O}$, then $x \cdot \mathfrak{a}^2,\ y \cdot \mathfrak{a}^3 \subseteq \mathcal{O}_K$ in terms of the integral ideal

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{e(\mathfrak{p})} \qquad \text{having exponents} \qquad e(\mathfrak{p}) = \left\lfloor \frac{v_{\mathfrak{p}}(p)}{p^{v_p(m)} - p^{v_p(m)-1}} \right\rfloor .$$

As a special case, Trygve Nagell in 1935 and Élisabeth Lutz in 1937 independently showed that when $K = \mathbb{Q}$ any torsion point $(x : y : 1) \in E(\mathbb{Q})$ satisfies (1) $4\,x$, $8\,y$ and $z = 2\,y + a_1\,x + a_3$ are rational integers, and (2) either $z = 0$ or z^2 divides $4\,\Delta$. Here are a couple of examples.

- The elliptic curve $E:\ y^2+x\,y=x^3+4\,x+1$ has $\Delta=-5^2\cdot13^2$. The only torsion point is $(x:y:1)=(-2:1:8)$, and it satisfies $4\,x=-1$, $8\,y=1$, and $z=2\,y+x=0$. Hence $E(\mathbb{Q})_{\text{tors}}=\big\{(-2:1:8),\,(0:1:0)\big\}\simeq Z_2$.
- The elliptic curve $E:\ y^2+y=x^3-x^2$ has $\Delta=-11$, so $z=2\,y+1$ must divide 2. Hence $E(\mathbb{Q})_{\text{tors}}=\big\{(0:0:1),\,(1:-1:1),\,(1:0:1),\,(0:-1:0),\,(0:1:0)\big\}\simeq Z_5$.

In general, since $E(\mathbb{C})$ is a torus, we have $E(\mathbb{C})_{\text{tors}}\simeq(\mathbb{Q}/\mathbb{Z})\times(\mathbb{Q}/\mathbb{Z})$. Hence we can find integers n and m such that $E(K)_{\text{tors}}\simeq Z_n\times Z_{nm}$. For instance, in two papers from 1977 and 1978, Barry Mazur showed that when $K=\mathbb{Q}$ we have $n\le2$ and $m\le12$.

Rank. Computing the rank r is much more difficult. Mordell's original idea was to consider the size of the index $\big[E(K):2\,E(K)\big]$. Since $E(K)\simeq Z_n\times Z_{nm}\times\mathbb{Z}^r$ for some integers n. m, and r, we have

$$\frac{E(K)}{2\,E(K)}\simeq\frac{Z_n}{{Z_n}^2}\times\frac{Z_{nm}}{{Z_{nm}}^2}\times\left(\frac{\mathbb{Z}}{2\,\mathbb{Z}}\right)^r=\begin{cases}{Z_2}^r & \text{if both } n \text{ and } m \text{ are odd,}\\ {Z_2}^{r+1} & \text{if } n \text{ is odd yet } m \text{ is even,}\\ {Z_2}^{r+2} & \text{if } n \text{ is even.}\end{cases}$$

Hence $\big|E(K):2\,E(K)\big|\le2^{r+2}$, so we can compute the rank by counting the number of cosets. We discuss these cases in detail.

Case #1: Rational Points of Order 2

Set-Up. Say that $n\,m$ is even, that is, $E(K)_{\text{tors}}$ has at least one K-rational point T of order 2. Since $[2]T=\mathcal{O}$, we see that $T=\big(2\,e\ :\ -a_1\,e-a_3\ :\ 2\big)$ where e is a K-rational root of the 2-division polynomial $\psi_2(x)=4\,x^3+b_2\,x^2+2\,b_4\,x+b_6$. With the substitutions

$$\begin{aligned}x'&=4\,\big(x-e\big)\\ y'&=4\,\big(2\,y+a_1\,x+a_3\big)\end{aligned}\qquad\text{and}\qquad\begin{aligned}a&=12\,e+b_2\\ b&=8\,\big(6\,e^2+b_2\,e+b_4\big)\end{aligned}$$

we find that $E:\ {y'}^2={x'}^3+a\,{x'}^2+b\,x'$ for some $a,\,b\in\mathcal{O}_K$. Note that the 2-torsion point $T\mapsto(0:0:1)$ under this substitution. To ease notation, we will simply write this elliptic curve as $y^2=x^3+a\,x+b$.

2-Isogenies. Our ultimate goal is to compute $\big|E(K):2\,E(K)\big|=2^{r+1}$ or 2^{r+2} depending on whether n is odd or even, so we use a trick. This curve admits two rational maps as follows.

$$\begin{array}{ccc}E':\ Y^2=X^3-2\,a\,X^2+(a^2-4\,b)\,X & & E:\ y^2=x^3+a\,x^2+b\,x\\ \big(X_1\ :\ X_2\ :\ X_0\big) & \xrightarrow{\ \varphi\ } & \big(2\,X_2^2\,X_0\ :\ X_2\,((a^2-4\,b)\,X_0^2-X_1^2)\ :\ 8\ X_1^2\,X_0\big)\\ \big(x_2^2\,x_0\ :\ x_2\,(b\,x_0^2-x_1^2)\ :\ x_1^2\,x_0\big) & \xleftarrow{\ \varphi'\ } & \big(x_1\ :\ x_2\ :\ x_0\big)\end{array}$$

These maps are actually dual 2-isogenies:

- $\varphi(P'\oplus Q')=\varphi(P')\oplus\varphi(Q')$ for all P' and Q' on E'.
- $\varphi'(P\oplus Q)=\varphi'(P)\oplus\varphi'(Q)$ for all P and Q on E.
- $E'(K)[\varphi]=\big\{(0:0:1),\,(0:1:0)\big\}$ is the kernel.
- $\varphi\circ\varphi'=[2]$ is the "multiplication-by-2" map on E.

This yields the short exact sequence

$$\{\mathcal{O}\} \longrightarrow \frac{E'(K)[\varphi]}{\varphi'\big(E(K)[2]\big)} \longrightarrow \frac{E'(K)}{\varphi'\big(E(K)\big)} \xrightarrow{\varphi} \frac{E(K)}{2\,E(K)} \longrightarrow \frac{E(K)}{\varphi\big(E'(K)\big)} \longrightarrow \{\mathcal{O}\}$$

It suffices then to compute

$$\big|E(K) : 2\,E(K)\big| = \frac{\big|E'(K) : \varphi'\big(E(K)\big)\big|\,\big|E(K) : \varphi\big(E'(K)\big)\big|}{\big|E'(K)[\varphi] : \varphi'\big(E(K)[2]\big)\big|}.$$

The denominator is easy to determine since it just involves a careful study of the points of order 2 in $E(K)_{\text{tors}}$:

$$\big|E'(K)[\varphi] : \varphi'\big(E(K)[2]\big)\big| = \begin{cases} 2 & \text{if } a^2 - 4\,b \notin (\mathcal{O}_K^\times)^2, \text{ that is, } n \text{ is odd;} \\ 1 & \text{if } a^2 - 4\,b \in (\mathcal{O}_K^\times)^2, \text{ that is, } n \text{ is even.} \end{cases}$$

In particular, $\big|E(K) : 2\,E(K)\big|\,\big|E'(K)[\varphi] : \varphi'\big(E(K)[2]\big)\big| = 2^{r+2}$ is independent of n.

Homogeneous Spaces. For the numerator, we introduce a new map:

$$\frac{E'(K)}{\varphi'\big(E(K)\big)} \times \frac{E(K)}{\varphi\big(E'(K)\big)} \longrightarrow \frac{K^\times}{(K^\times)^2} \times \frac{K^\times}{(K^\times)^2}$$

$$\big((X_1 : X_2 : X_0),\quad (x_1 : x_2 : x_0)\big) \longrightarrow \big(X_1\,X_0 \bmod (K^\times)^2,\quad x_1\,x_0 \bmod (K^\times)^2\big)$$

This is actually an injective group homomorphism whose image consists of those (d, d') such that

- d is square-free and divides b, while d' is square-free and divides $a^2 - 4\,b$ in $\mathcal{O}_K$.
- The quartic curve $C_d : w^2 = d + a\,z^2 + (b/d)\,z^4$ has a K-rational point $(z : w : 1)$.
- The quartic curve $D_{d'} : W^2 = d' - 2\,a\,Z^2 + (a^2 - 4\,b)/d'\,Z^4$ has a K-rational point $(Z : W : 1)$.

The curves C_d and $D_{d'}$ are principal homogeneous spaces. The number of such pairs (d, d') is 2^{r+2} in terms of the desired rank r. Computing the various divisors of b and $a^2 - 4\,b$ in $\mathcal{O}_K$ is not difficult, but finding K-rational points $(z : w : 1)$ and $(Z : W : 1)$ is. Conversely, given such points on these principal homogeneous spaces, we can find K-rational points $(X_1 : X_2 : X_0)$ and $(x_1 : x_2 : x_0)$. For example, we have a commutative diagram in the form

$$\begin{array}{ccc} E' : Y^2 = X^3 - 2\,a\,X^2 + (a^2 - 4\,b)\,X & \longrightarrow & E : y^2 = x^3 + a\,x^2 + b\,x \\ \big\updownarrow & \nearrow & \\ C_d : w^2 = d + a\,z^2 + (b/d)\,z^4 & & \end{array}$$

defined by the maps

$$\begin{array}{ccc} (X_1 : X_2 : X_0) & \longmapsto & (x_1 : x_2 : x_0) \\ \big\updownarrow & & \| \\ (z_1 : z_2 : z_0) & & \big(d\,z_1\,z_0^2 \;:\; d\,z_2\,z_0^2 \;:\; z_1^3\big) \\ \| & & \| \\ \big(2\,\sqrt{d}\,X_1\,X_2\,X_0 \;:\; \sqrt{d}\,X_1\,((a^2 - 4\,b)\,X_0^2 - X_1^2) \;:\; X_2^2\,X_0\big) & & \big(2\,X_2^2\,X_0 \;:\; X_2\,((a^2 - 4\,b)\,X_0^2 - X_1^2) \;:\; 8\,X_1^2\,X_0\big) \end{array}$$

Example. Consider the elliptic curve $E : y^2 + x\,y = x^3 + 4\,x + 1$. We found before that the curve has torsion subgroup $E(\mathbb{Q})_{\text{tors}} = \big\{(-2 : 1 : 8),\, (0 : 1 : 0)\big\} \simeq Z_2$. On the other hand, the rank r satisfies

$$2^{r+2} = \big|E'(\mathbb{Q}) : \varphi'\big(E(\mathbb{Q})\big)\big|\,\big|E(\mathbb{Q}) : \varphi\big(E'(\mathbb{Q})\big)\big|$$

in terms of the 2-isogeneous elliptic curve $E' : Y^2 = X^3 + X^2 - 16\,X$. We focus on square-free divisors d of 65 and square-free divisors d' of 16, and search for $\mathbb{Q}$-rational points on the principal homogeneous spaces

$$C_d : \quad w^2 = d - 2\,z^2 + \frac{65}{d}\,z^4 \qquad \text{and} \qquad D_{d'} : \quad W^2 = d' + Z^2 - \frac{16}{d'}\,Z^4.$$

For example, $C_{-1}(\mathbb{R}) = \emptyset$, and hence C_{-1} has no $\mathbb{Q}$-rational points. Similarly, using the `MAGMA` online calculator `http://magma.maths.usyd.edu.au/calc/` along with the following commands:

```
> P<Z> := PolynomialRing(Rationals());
> d := 2;
> D := HyperellipticCurve(d + Z^2 - (16/d)*Z^4);
> IsLocallySolvable(D,2);
false
```

we find that $D_{\pm 2}(\mathbb{Q}_2) = \emptyset$, and hence $D_{\pm 2}$ has no $\mathbb{Q}$-rational points. We summarize all of this in the following table.

Divisor d	Point $(z : w : 1)$
-65	None over $\mathbb{R}$
-13	None over $\mathbb{R}$
-5	None over $\mathbb{R}$
-1	None over $\mathbb{R}$
$+1$	$(0 : 1 : 1)$
$+5$	$(1 : 4 : 1)$
$+13$	$(1 : 4 : 1)$
$+65$	$(1 : 8 : 1)$

Divisor d'	Point $(Z : W : 1)$
-2	None over $\mathbb{Q}_2$
-1	$(1 : 4 : 1)$
$+1$	$(0 : 1 : 1)$
$+2$	None over $\mathbb{Q}_2$

Hence we find the indices $\big|E'(\mathbb{Q}) : \varphi'\big(E(\mathbb{Q})\big)\big| = 4$ and $\big|E(\mathbb{Q}) : \varphi\big(E'(\mathbb{Q})\big)\big| = 2$, so that $2^{r+2} = \big|E(K) : 2\,E(K)\big|\,\big|E'(K)[\varphi] : \varphi'\big(E(K)[2]\big)\big| = 8$. We may conclude that $r = 1$. In fact, we have a rational map

$$\begin{aligned} C_d : w^2 = d - 2\,z^2 + \frac{65}{d} \quad &\longrightarrow \qquad E : y^2 + x\,y = x^3 + 4\,x + 1 \\ \big(z \;:\; w \;:\; 1\big) \quad &\longrightarrow \big(2\,d\,z - 2\,z^3 \;:\; d\,w - d\,z + z^3 \;:\; 8\,z^3\big) \end{aligned}$$

so that the $\mathbb{Q}$-rational point $(z : w : 1) = (1 : 4 : 1)$ on C_5 yields the $\mathbb{Q}$-rational point of infinite order $(x : y : 1) = (1 : -3 : 1)$ on E. With just a bit more work, we may conclude that $E(\mathbb{Q}) \simeq Z_2 \times \mathbb{Z}$ as generated by $(-2 : 1 : 8)$ and $(1 : -3 : 1)$.

Case #2: No Rational Points of Order 2

Set-Up. Say that $n\,m$ is odd, that is, $E(K)_{\text{tors}}$ has no K-rational points of order 2. Our ultimate goal is to compute $\big|E(K) : 2\,E(K)\big| = 2^r$. We will show there exists a finite extension L/K such that we have the following diagram:

$$\begin{array}{ccccc} \dfrac{E(K)}{2\,E(K)} & \xrightarrow{\ \hookrightarrow\ } & \left\{ x \in \mathrm{Sel}^{(2)}(U_S/L) \,\middle|\, \mathbb{N}_{L/K}(x) \in \left(K^\times\right)^2 \right\} & \xrightarrow{\ \hookrightarrow\ } & \mathrm{Sel}^{(2)}(U_S/L) \\ & & \Big\downarrow & & \Big\downarrow \\ & & \left\{ \mathfrak{a} \in C\ell(\mathcal{O}_{L,S})[2] \,\middle|\, \mathbb{N}_{L/K}\,\mathfrak{a} \in P(\mathcal{O}_{K,S}) \right\} & \xrightarrow{\ \hookrightarrow\ } & C\ell(\mathcal{O}_{L,S})[2] \end{array}$$

In the process, we will explain all of the notation.

Ideal Class Group. Let S be a finite set of primes of K containing the infinite places of K, and L be a finite extension of K which is unramified outside of S. In practice, S is the set of places of K containing all of the archimedean places, all places dividing 2, and all places which divide the discriminant Δ; while $L = K[x]/(\psi_2(x))$ in terms of the 2-division polynomial $\psi_2(x) = 4\,x^3 + b_2\,x^2 + 2\,b_4\,x + b_6$. Since the discriminant of $\psi_2(x)$ is Δ, we see that L/K is a cubic extension which is unramified outside of S.

Let me recall some facts about the class group $C\ell(\mathcal{O}_{L,S})$. Recall that the S-integers of L is the ring

$$\mathcal{O}_{L,S} = \left\{ x \in L \;\middle|\; \mathrm{ord}_{\mathfrak{P}}(x) \geq 0 \text{ for all } \mathfrak{P} \text{ lying over } \mathfrak{p} \notin S \right\},$$

and the S-units of L is the group $U_S(L) = \mathcal{O}_{L,S}^\times$. A fractional ideal $\mathfrak{a}$ of $\mathcal{O}_{L,S}$ is an $\mathcal{O}_{L,S}$-submodule of L such that $x\,\mathfrak{a} \subseteq \mathcal{O}_{L,S}$ for some nonzero $x \in \mathcal{O}_{L,S}$; denote $I(\mathcal{O}_{L,S})$ as the collection of such nonzero ideals. Similarly, denote $P(\mathcal{O}_{L,S}) \subseteq I(\mathcal{O}_{L,S})$ as the collection of nonzero principal fractional ideals $\mathfrak{a} = x\,\mathcal{O}_{L,S}$ for nonzero $x \in L$. It is well-known that

- $\mathcal{O}_{L,S}$ is a Dedekind domain.
- $I(\mathcal{O}_{L,S})$ forms a group under multiplication, $P(\mathcal{O}_{L,S})$ forms a subgroup, and every nonzero fractional ideal $\mathfrak{a} \in I(\mathcal{O}_{L,S})$ can be uniquely factored into a product of prime ideals $\mathfrak{P}$.
- The ideal class group $C\ell(\mathcal{O}_{L,S}) = I(\mathcal{O}_{L,S})/P(\mathcal{O}_{L,S})$ is a finite abelian group.

Selmer Group. Consider the following multiplicative groups:

$$\mathrm{Vir}^{(m)}(U_S/L) = \left\{ x \in L^\times \;\middle|\; \mathrm{ord}_{\mathfrak{P}}(x) \equiv 0 \pmod{m} \text{ for all } \mathfrak{P} \text{ lying over } \mathfrak{p} \notin S \right\},$$

$$\mathrm{Sel}^{(m)}(U_S/L) = \left\{ x \in \frac{L^\times}{\left(L^\times\right)^m} \;\middle|\; \mathrm{ord}_{\mathfrak{P}}(x) \equiv 0 \pmod{m} \text{ for all } \mathfrak{P} \text{ lying over } \mathfrak{p} \notin S \right\}.$$

When $S = \emptyset$, Henri Cohen uses slightly different notation in his book *Advanced Topics in Computational Number Theory*. He calls the set $V_m(L) = \mathrm{Vir}^{(m)}(U_\emptyset/L)$ the "virtual units" of L, and $S_m(L) = V_m(L)/(L^\times)^m = \mathrm{Sel}^{(m)}(U_\emptyset/L)$ the m-Selmer group.

We have a well-defined morphism $\mathrm{Vir}^{(m)}(U_S/L) \to I(\mathcal{O}_{L,S})$ which sends x to the nonzero fractional ideal $\mathfrak{a} = \prod_{\mathfrak{p} \notin S} \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e(x,\mathfrak{P})}$ in terms of the exponents $e(x,\mathfrak{P}) = \mathrm{ord}_{\mathfrak{P}}(x)/m$. Since $\mathfrak{a}^m = x\,\mathcal{O}_{L,S}$ is a principal ideal, we have the following diagram:

$$\begin{array}{ccccccccc}
 & & \{1\} & & \{1\} & & \{1\} & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\{1\} & \longrightarrow & \left(\mathcal{O}_{L,S}^{\times}\right)^m & \longrightarrow & U_S(L) & \longrightarrow & \dfrac{U_S(L)}{U_S(L)^m} & \longrightarrow & \{1\} \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\{1\} & \longrightarrow & \left(L^{\times}\right)^m & \longrightarrow & \mathrm{Vir}^{(m)}(U_S/L) & \longrightarrow & \mathrm{Sel}^{(m)}(U_S/L) & \longrightarrow & \{1\} \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\{1\} & \longrightarrow & P(\mathcal{O}_{L,S}) & \longrightarrow & \left\{ \mathfrak{a} \in I(\mathcal{O}_{L,S}) \,\middle|\, \mathfrak{a}^m \in P(\mathcal{O}_{L,S}) \right\} & \longrightarrow & C\ell(\mathcal{O}_{L,S})[m] & \longrightarrow & \{1\} \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \{1\} & & \{1\} & & \{1\} & &
\end{array}$$

We conclude that we have the following short-exact sequence:

$$\{1\} \longrightarrow \frac{U_S(L)}{U_S(L)^m} \longrightarrow \mathrm{Sel}^{(m)}(U_S/L) \longrightarrow C\ell(\mathcal{O}_{L,S})[m] \longrightarrow \{1\}.$$

This is a generalization of Proposition 5.2.8 in Henri Cohen's book *Advanced Topics in Computational Number Theory*. We view $\mathrm{Sel}^{(m)}(U_S/L)$ as the m-Selmer group of the S-units $U_S(L) = \mathcal{O}_{L,S}^{\times}$ of L, and the subgroup $C\ell(\mathcal{O}_{L,S})[m]$ as the m-torsion in the class group of $\mathcal{O}_{L,S}$. Note that $\mathrm{Sel}^{(m)}(U_S/L)$ is the intersection of the kernels $L^{\times}/(L^{\times})^m \to L_{\mathfrak{P}}^{\times}/(L_{\mathfrak{P}}^{\times})^m$ for $\mathfrak{P} \in \mathrm{mSpec}\,\mathcal{O}_{L,S}$. This is meant to look similar to the short exact sequence

$$\{\mathcal{O}\} \longrightarrow \frac{E(L)}{m\,E(L)} \longrightarrow \mathrm{Sel}^{(m)}(E/L) \longrightarrow Ш(E/L)[m] \longrightarrow \{0\}$$

for elliptic curves, where $\mathrm{Sel}^{(m)}(E/L)$ is the m-Selmer group of E, and $Ш(E/L)[m]$ is the m-torsion in the Shafarevich-Tate group of E. For this reason, we may consider the class group $C\ell(\mathcal{O}_{L,S})$ to be the Shafarevich-Tate group $Ш(U_S/L)$ of the collection of S-units of L.

Application to Ranks of Elliptic Curves. We will specialize to the case where $m = 2$. Assume that

- K is a number field.
- $E : y^2 + a_1\,x\,y + a_3\,y = x^3 + a_2\,x^2 + a_4\,x + a_6$ is an elliptic curve over K such that the 2-division polynomial $\psi_2(x) = 4\,x^3 + b_2\,x^2 + 2\,b_4\,x + b_6$ is irreducible over K.
- S is the set of places of K containing all of the archimedean places, all places dividing 2, and all places which divide the discriminant Δ.
- $L = K(e) \simeq K[x]/(\psi_2(x))$ is that cubic extension of K found by adjoining one root of the 2-division polynomial.

We will show

$$2^r = \big|E(K) : 2\,E(K)\big| \le \big|\mathrm{Sel}^{(2)}(U_S/L)\big| = \big|U_S(L) : U_S(L)^2\big|\,\big|C\ell(\mathcal{O}_{L,S})[2]\big|.$$

Actually, we may conclude something stronger. Indeed, fix $T = \big(2\,e \;:\; -a_1\,e - a_3 \;:\; 2\big)$ as a 2-torsion point defined over L, and define the map $f_T : E(K) \to L^\times$ which sends $P = (x : y : 1)$ to $x - e \bmod (L^\times)^2$. This induces the diagram

$$\begin{array}{ccccc}
 & & \{1\} & & \{1\} \\
 & & \downarrow & & \downarrow \\
 & & \left\{ x \in \dfrac{U_S(L)}{U_S(L)^2} \,\middle|\, \mathbb{N}_{L/K}(x) \in \big(\mathcal{O}_{K,S}^\times\big)^2 \right\} & \xrightarrow{\;\hookrightarrow\;} & \dfrac{U_S(L)}{U_S(L)^2} \\
 & & \downarrow & & \downarrow \\
\dfrac{E(K)}{2\,E(K)} & \xrightarrow{\;\hookrightarrow\;} & \left\{ x \in \mathrm{Sel}^{(2)}(U_S/L) \,\middle|\, \mathbb{N}_{L/K}(x) \in \big(K^\times\big)^2 \right\} & \xrightarrow{\;\hookrightarrow\;} & \mathrm{Sel}^{(2)}(U_S/L) \\
 & & \downarrow & & \downarrow \\
 & & \left\{ \mathfrak{a} \in C\ell(\mathcal{O}_{L,S})[2] \,\middle|\, \mathbb{N}_{L/K}\,\mathfrak{a} \in P(\mathcal{O}_{K,S}) \right\} & \xrightarrow{\;\hookrightarrow\;} & C\ell(\mathcal{O}_{L,S})[2] \\
 & & \downarrow & & \downarrow \\
 & & \{1\} & & \{1\}
\end{array}$$

It suffices to show that the horizontal maps are injective, that is, $f_T(P) \bmod (L^\times)^2$ is trivial if and only if $P \in 2\,E(K)$. Observe the identity

$$g_T(P) = \frac{4\,e^2 + b_2\,e + b_4 + 4\,e\,x - 2\,x^2}{2\,(2\,y + a_1\,x + a_3)} \qquad \Longrightarrow \qquad g_T(P)^2 = \big(f_T \circ [2]\big)(P).$$

If $P = [2]X$ for some $X \in E(K)$, then $\sqrt{f_T(P)} = g_T(X) \in L^\times$. Conversely, write $\sqrt{f_T(P)} = r + s\,e + t\,e^2$ as an element of $L = K(e)$ for some r, s, $t \in K$, and define the point

$$X = \Big(8\,s - 2\,(a_1^2 + 4\,a_2)\,t \;:\; -4\,a_1\,s + (a_1^3 + 4\,a_1\,a_2 - 4\,a_3)\,t \pm 8 \;:\; 8\,t\Big).$$

As $\big(r + s\,e + t\,e^2\big)^2 = x - e$ has no e^2 term, we have $r = \big(-16\,s^2 + 8\,b_2\,s\,t + (8\,b_4 - b_2^2)\,t^2\big)/\big(32\,t\big)$. It is easy to verify that $X \in E(K)$ and $P = [\pm 2]X$.

This diagram induces the group homomorphism $E(K)/2\,E(K) \to C\ell(\mathcal{O}_{L,S})[2]$ which sends a K-rational point $P = (x : y : 1)$ to the fractional ideal

$$\mathfrak{a} = \prod_{\mathfrak{p} \notin S} \prod_{\mathfrak{P} \mid \mathfrak{p}} \mathfrak{P}^{e(P,\mathfrak{P})} \qquad \text{where} \qquad e(P,\mathfrak{P}) = \frac{\mathrm{ord}_{\mathfrak{P}}(x - e)}{2}.$$

Moreover, using Minkowski's Bound, we see that representatives $\mathfrak{a} \in I(\mathcal{O}_{L,S})$ of the cosets $C\ell(\mathcal{O}_{L,S}) = I(\mathcal{O}_{L,S})/P(\mathcal{O}_{L,S})$ satisfy the following:

- $\mathfrak{a}^2 = (x - e)\,\mathcal{O}_{L,S}$ and $\mathbb{N}_{L/K}\,\mathfrak{a} = y\,\mathcal{O}_{K,S}$ are principal ideals.
- $\mathbb{N}_{L/K}\,\mathfrak{a} = \prod_{\mathfrak{p} \notin S} \mathfrak{p}^{e(\mathfrak{p})}$ does not involve primes $\mathfrak{p} \in S$.
- $\mathbb{N}_{L/\mathbb{Q}}\,\mathfrak{a} \le \sqrt{|\mathrm{Disc}(\mathcal{O}_L)|}\,(n!/n^n)\,(4/\pi)^{r_2}$ where $n = [L : \mathbb{Q}] = r_1 + 2\,r_2$.

In practice, $K = \mathbb{Q}$, so that $L = \mathbb{Q}(e)$ is an extension of degree $n = 3$. The Minkowski Bound is either $M_L = (n!/n^n)\,(4/\pi)^{r_2} = 2/9$ or $8/(9\pi)$ for cubic extensions L/K, so it should be relatively easy to find ideals $\mathfrak{a}$ of $\mathcal{O}_L$ satisfying these properties.

Examples. For each rational number t, consider the elliptic curve

$$E_t: \quad y\,(y+1) = x\,(x+1)\,(x+t).$$

It is easy to check that its 2-division polynomial is $\psi_2(x) = 4\,x^3 + 4\,(t+1)\,x^2 + 4\,t\,x + 1$. William Stein has observed that the first few values of t give some well-known elliptic curves:

t	Elliptic Curve E_t	Cremona Label	Δ	Bad Primes S	$E_t(\mathbb{Q})_{\text{tors}}$	Rank of E_t
1	$y^2 + y = x^3 - x^2$	11.a3	-11	$\{-1,\, 2,\, 11\}$	Z_5	0
2	$y^2 + y = x^3 - x$	37.a1	37	$\{-1,\, 2,\, 37\}$	Z_1	1
3	$y^2 + y = x^3 + x^2 - 2\,x$	389.a1	389	$\{-1,\, 2,\, 389\}$	Z_1	2
5	$y^2 + y = x^3 - 7\,x + 6$	5077.a1	5077	$\{-1,\, 2,\, 5077\}$	Z_1	3

We have already seen how to use the theorem of Lutz and Nagell to compute the torsion subgroups. We discuss how one computes the rank $r = r(t)$ of these curves. The idea is to count $\big|E(K) : 2\,E(K)\big| = 2^r$ using the embedding $f_T : E_t(\mathbb{Q})/2\,E_t(\mathbb{Q}) \hookrightarrow \text{Sel}^{(2)}(U_S/L)$.

The first step is to find a basis for the integral closure $\mathcal{O}_L$ of $\mathbb{Z}$ in $L = \mathbb{Q}(e)$. We find the following information.

t	$\psi_2(e)$	$L = \mathbb{Q}(\varepsilon)$	$\mathcal{O}_L = \mathbb{Z}[\varepsilon]$	$\text{Disc}(\mathcal{O}_L)$	$\sqrt{\lvert\text{Disc}(\mathcal{O}_L)\rvert}$ $\cdot\,(n!/n^n)\,(4/\pi)^{r_2}$
1	$4\,e^3 - 4\,e^2 + 1$	$\varepsilon^3 - \varepsilon^2 - \varepsilon - 1$	$\varepsilon = 1 - 2\,e$	$-2^2 \cdot 11$	1.877
2	$4\,e^3 - 4\,e + 1$	$\varepsilon^3 - 3\,\varepsilon^2 - \varepsilon + 1$	$\varepsilon = 1 - 2\,e$	$2^2 \cdot 37$	2.703
3	$4\,e^3 + 4\,e^2 - 8\,e + 1$	$\varepsilon^3 - 8\,\varepsilon^2 + 12\,\varepsilon - 2$	$\varepsilon = 2 - 2\,e$	$2^2 \cdot 389$	8.766
5	$4\,e^3 - 28\,e + 25$	$\varepsilon^3 - 6\,\varepsilon^2 - 16\,\varepsilon - 2$	$\varepsilon = 2 - 2\,e$	$2^2 \cdot 5077$	31.668

The next step is to use the Minkowski Bound to compute the class number $h(L) = \big|C\ell(\mathcal{O}_L)\big|$. We seek all ideals $\mathfrak{a}$ satisfying $\mathbb{N}_{L/\mathbb{Q}}\,\mathfrak{a} \le \sqrt{\lvert\text{Disc}(\mathcal{O}_L)\rvert}\,(n!/n^n)\,(4/\pi)^{r_2}$. If all such ideals are principal, then $h(L) = 1$. For example, we can generate prime ideals using the following `Sage` commands:

```
sage: L = NumberField(x^3 - 6*x^2 - 16*x - 2, 'epsilon')
sage: O = L.maximal_order()
sage: a = 5*O
sage: a.prime_factors()
[
 Fractional ideal (5, epsilon^2 - 9*epsilon - 4),
 Fractional ideal (5, epsilon - 2)
]
```

We find that

$$C\ell(\mathcal{O}_L) = \begin{cases} \{\mathcal{O}_L\} & \text{if } t = 1,\, 2,\, 3, \\ \{\mathcal{O}_L,\, \mathfrak{P}_5\} & \text{if } t = 5; \end{cases} \qquad \Longrightarrow \qquad h(L) = \begin{cases} 1 & \text{if } t = 1,\, 2,\, 3, \\ 2 & \text{if } t = 5. \end{cases}$$

We summarize the relevant data in the following table.

t	Ideal $\mathfrak{a} \in I(\mathcal{O}_L)$	$\mathbb{N}_{L/\mathbb{Q}}\,\mathfrak{a}$	Relations
1	$\mathcal{O}_L$	1	–
2	$\mathcal{O}_L$	1	–
	$\mathfrak{P}_2 = (\varepsilon - 1)\,\mathcal{O}_L$	2	
3	$\mathcal{O}_L$	1	–
	$\mathfrak{P}_2 = \varepsilon\,\mathcal{O}_L$	2	
	$\mathfrak{P}_3 = (\varepsilon - 1)\,\mathcal{O}_L$	3	
	${\mathfrak{P}_2}^2 = \varepsilon^2\,\mathcal{O}_L$	4	
	$\mathfrak{P}_2\,\mathfrak{P}_3 = \varepsilon\,(\varepsilon - 1)\,\mathcal{O}_L$	6	
	${\mathfrak{P}_2}^3 = 2\,\mathcal{O}_L$	8	
5	$\mathcal{O}_L$	1	
	$\mathfrak{P}_2 = \varepsilon\,\mathcal{O}_L$	2	
	${\mathfrak{P}_2}^2 = \varepsilon^2\,\mathcal{O}_L$	4	
	$\mathfrak{P}_5$	5	$\mathfrak{P}_5\,\mathfrak{P}_7 = (\varepsilon^2 - 9\,\varepsilon - 1)\,\mathcal{O}_L$
	$\mathfrak{P}_7,\, \mathfrak{Q}_7,\, \mathfrak{R}_7 = (\varepsilon + 1)\,\mathcal{O}_L$	7	$\mathfrak{P}_7\,\mathfrak{Q}_7 = (\varepsilon^2 - 7\,\varepsilon - 9)\,\mathcal{O}_L$
	${\mathfrak{P}_2}^3 = 2\,\mathcal{O}_L$	8	
	$\mathfrak{P}_2\,\mathfrak{P}_5$	10	
	$\mathfrak{P}_{11}$	11	$\mathfrak{P}_5\,\mathfrak{P}_{11} = (\varepsilon^2 + \varepsilon - 1)\,\mathcal{O}_L$
	$\mathfrak{P}_{13}$	13	$\mathfrak{P}_5\,\mathfrak{P}_{13} = (5\,\varepsilon^2 - 7\,\varepsilon - 1)\,\mathcal{O}_L$
	$\mathfrak{P}_2\,\mathfrak{P}_7,\, \mathfrak{P}_2\,\mathfrak{Q}_7,\, \mathfrak{P}_2\,\mathfrak{R}_7 = \varepsilon\,(\varepsilon + 1)\,\mathcal{O}_L$	14	
	${\mathfrak{P}_2}^4 = 2\,\varepsilon\,\mathcal{O}_L$	16	
	$\mathfrak{P}_{17}$	17	$\mathfrak{P}_5\,\mathfrak{P}_{17} = (\varepsilon^2 - 8\,\varepsilon - 3)\,\mathcal{O}_L$
	${\mathfrak{P}_2}^2\,\mathfrak{P}_5$	20	
	$\mathfrak{P}_2\,\mathfrak{P}_{11}$	22	
	$\mathfrak{P}_{23} = (\varepsilon - 1)\,\mathcal{O}_L$	23	
	$\mathfrak{Q}_5,\, {\mathfrak{P}_5}^2 = (2\,\varepsilon^2 + 8\,\varepsilon + 1)\,\mathcal{O}_L$	25	$\mathfrak{P}_5\,\mathfrak{Q}_5 = 5\,\mathcal{O}_L$
	$\mathfrak{P}_2\,\mathfrak{P}_{13}$	26	
	$\mathfrak{P}_3 = 3\,\mathcal{O}_L$	27	
	${\mathfrak{P}_2}^2\,\mathfrak{P}_7,\, {\mathfrak{P}_2}^2\,\mathfrak{Q}_7,\, {\mathfrak{P}_2}^2\,\mathfrak{R}_7 = (\varepsilon^2 - 8\,\varepsilon - 2)\,\mathcal{O}_L$	28	
	$\mathfrak{P}_{29}$	29	$\mathfrak{P}_5\,\mathfrak{P}_{29} = (\varepsilon^2 - 4\,\varepsilon - 1)\,\mathcal{O}_L$
	$\mathfrak{P}_{31}$	31	$\mathfrak{P}_5\,\mathfrak{P}_{31} = (\varepsilon^2 - 5\,\varepsilon - 7)\,\mathcal{O}_L$

Relative to the 2-torsion point $T = \big(2\,e\,:\,-a_1\,e - a_3\,:\,2\big)$, the final step is to compute the image of the maps $f_T : E_t(\mathbb{Q})/2\,E_t(\mathbb{Q}) \hookrightarrow \mathrm{Sel}^{(2)}(U_S/L)$ sending $P = (x : y : 1)$ to $f_T(P) = x - e \bmod (L^\times)^2$ and $\mathrm{Sel}^{(2)}(U_S/L) \twoheadrightarrow C\ell(\mathcal{O}_{L,S})[2]$ sending $x - e$ to $\mathfrak{a}$ where $\mathfrak{a}^2 = (x - e)\,\mathcal{O}_{L,S}$. Using the `Sage` commands

```
sage: L = NumberField(x^3 - 8*x^2 + 12*x - 2, 'epsilon')
sage: L.units()
```

```
[
 epsilon^2 - 6*epsilon + 1,
 2*epsilon^2 - 4*epsilon + 1
]
```

we may compare these with elements u in $\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2$ such that $\mathbb{N}_{L/\mathbb{Q}}\,u$ is in $\left(\mathbb{Z}^\times\right)^2 = \{1\}$.

t	$u \in \mathcal{O}_L^\times$ with $\mathbb{N}_{L/\mathbb{Q}}\,u = 1$	$P \in E_t(\mathbb{Q})$	$f_T(P) \in \mathrm{Sel}^{(2)}(U_S/L)$	$\mathfrak{a} \in I(\mathcal{O}_L)$
1	$\langle \varepsilon \rangle$	$(0:0:1)$	1	$\mathcal{O}_L$
2	$\langle -\varepsilon,\, 2\,\varepsilon - 1 \rangle$	$(0:0:1)$	$2\,\varepsilon - 1$	$\mathcal{O}_L$
3	$\langle \varepsilon^2 - 6\,\varepsilon + 1,\, 3\,\varepsilon^2 - 6\,\varepsilon + 1 \rangle$	$(-1:1:1)$ $(0:0:1)$	$\varepsilon^2 - 6\,\varepsilon + 1$ $3\,\varepsilon^2 - 6\,\varepsilon + 1$	$\mathcal{O}_L$ $\mathcal{O}_L$
5	$\langle 4\,\varepsilon^2 + 8\,\varepsilon + 1,\, -\varepsilon^2 + 8\,\varepsilon + 1 \rangle$	$(-2:3:1)$ $(-1:3:1)$ $(0:2:1)$	$-\varepsilon^2 + 8\,\varepsilon + 1$ $3\,\varepsilon^2 + 2\,\varepsilon - 7$ $2\,\varepsilon^2 + 8\,\varepsilon + 1$	$\mathcal{O}_L$ $\mathfrak{P}_7$ $\mathfrak{P}_5$

We conclude that

$$\left|E(K) : 2\,E(K)\right| \geq \begin{cases} 1 & \text{if } t = 1, \\ 2 & \text{if } t = 2, \\ 4 & \text{if } t = 3, \\ 8 & \text{if } t = 5; \end{cases} \qquad \text{while} \qquad \left|\mathcal{O}_L^\times : \left(\mathcal{O}_L^\times\right)^2\right| \left|C\ell(\mathcal{O}_L)[2]\right| = \begin{cases} 2 & \text{if } t = 1, \\ 4 & \text{if } t = 2, \\ 4 & \text{if } t = 3, \\ 8 & \text{if } t = 5. \end{cases}$$

Since $2^r = \left|E(K) : 2\,E(K)\right| \leq \left|\mathcal{O}_L^\times : \left(\mathcal{O}_L^\times\right)^2\right| \left|C\ell(\mathcal{O}_L)[2]\right|$, we have the inequalities

$$\begin{aligned} 0 \leq r \leq 1 \qquad & \text{if } t = 1, \\ 1 \leq r \leq 2 \qquad & \text{if } t = 2, \\ r = 2 \qquad & \text{if } t = 3, \\ r = 3 \qquad & \text{if } t = 5. \end{aligned}$$

Thus far we have only used information about the rings $\mathcal{O}_{L,S}$ to obtain upper bounds for the ranks of $E_t(\mathbb{Q})$. We could determine the rank exactly when $t = 1$ and $t = 2$ if we could determine whether the units $\pm\varepsilon \in \mathrm{Sel}^{(2)}(U_S/L)$ lie in the image of maps f_T. This will require us to use more specific information about the elliptic curves E_t.