

Elliptic Curves (Math 7280), Fall 2004 (with H. Verrill)

Notes on Selmer's example of the failure of the Hasse principle for genus 1 curves. (Following Cassels Chapter 18, adding a few more details and pictures.)

Selmer showed that the projective curve

$$C : F(X, Y, Z) := 3X^3 + 4Y^3 + 5Z^3 = 0$$

has points over \mathbf{Q}_p for all primes p , and in \mathbf{R} , but no rational points. (Selmer did a big study of equations of this form in the 1950s [Selmer, E, *The Diophantine equation $ax^3 + by^3 + cz^3 = 0$* . Acta Math. 85, (1951). 203-362]. Later we will define Selmer's group.)

1 C has points everywhere locally

1.1 C has points over finite fields

Later on we will see that any smooth cubic curve over a finite field \mathbf{F}_q has at least one point over \mathbf{F}_q . In fact we have the following result, which for now we'll use without proof (see Chapter 25).

Theorem 1.1 (Hasse). *If E is a smooth elliptic curve defined over a finite field \mathbf{F}_q , (where $\#\mathbf{F}_q = q$, $q = p^n$ for a prime p , and $n \in \mathbf{N}$) then*

$$|\#E(\mathbf{F}_q) - q - 1| \leq 2\sqrt{q}.$$

Corollary 1.2. *If E is a smooth elliptic curve over \mathbf{F}_p , E has at least $(\sqrt{p} - 1)^2$ points.*

proof: $\#E(\mathbf{F}_q) \geq q + 1 - |\#E(\mathbf{F}_q) - q - 1| \geq q + 1 - 2\sqrt{q} = (\sqrt{q} - 1)^2 > 0$.

Corollary 1.3. *If $p > 5$ is a prime, $C(\mathbf{F}_p) \neq \emptyset$.*

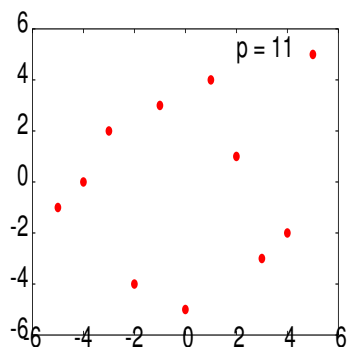
Proof.

$$\frac{\partial F}{\partial X} = 9X^2, \quad \frac{\partial F}{\partial Y} = 12Y^2, \quad \frac{\partial F}{\partial Z} = 15Z^2.$$

A point is smooth unless all of these are zero. If $p > 0$, this can only happen at $(0 : 0 : 0)$, but this is not a point of projective space, so $C(\mathbf{F}_p)$ is smooth for $p > 0$. Now the above corollary applies. □

Lemma 1.4. *If $p = 2, 3, 5$ then $C(\mathbf{F}_p) \neq \emptyset$.*

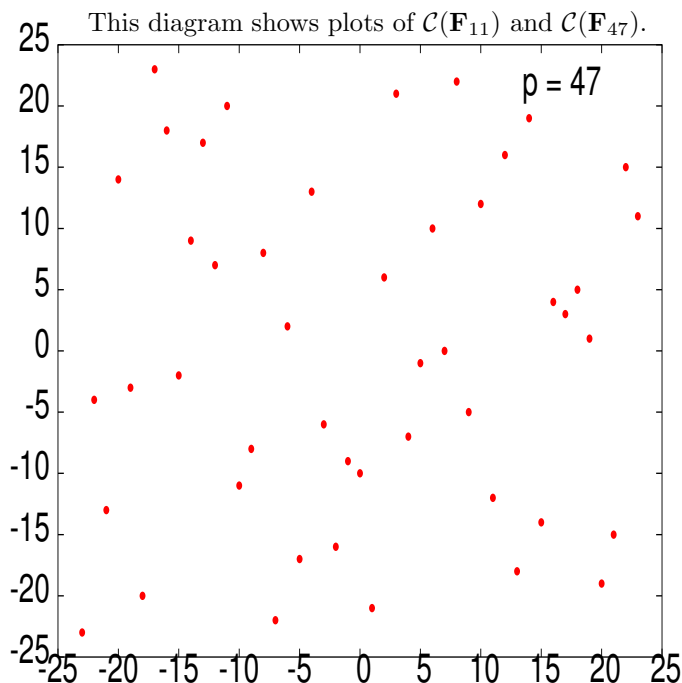
Proof. $(3 : 1 : 1) \in C(\mathbf{F}_p)$ for $p = 2, 3, 5$. □



Example point counts:

p	$\#C(\mathbf{F}_p)$
2	3
3	4
5	6
7	1
11	12
13	10

Question:
How does $\#C(\mathbf{F}_p)$ vary as p varies?



1.2 \mathcal{C} has points over p -adic fields.

Recall Hensel's lemma, (from Chapter 10; a version of Newton's method):

Theorem 1.5 (Hensel). *If $F(x) \in \mathbf{Z}_p[x]$, and there is a $t \in \mathbf{Z}$ with $|F(t)|_p < 1$ and $|F'(t)|_p = 1$, then t can be lifted (i.e., $t \equiv r \pmod{p}$) to a solution $r \in \mathbf{Z}_p$ with $F(r) = 0$.*

Corollary 1.6 (of corollary 1.3). *For a prime $p > 5$, $\#\mathcal{C}(\mathbf{Q}_p) \neq 0$.*

Proof. Suppose $(a : b : c)$ is a point on $\mathcal{C}(\mathbf{F}_p)$. Take $a, b, c \in \mathbf{Z}$, with $\gcd(a, b, c) = 1$. So one of a, b, c is not divisible by p . Suppose $p \nmid a$, then let $G(T) = 3X^3 + 4b^3 + 5c^3$. Then check that $G(a)$ and $G'(a)$ satisfy the requirements to apply Hensel's lemma. Similarly for $p \nmid b$ or $p \nmid c$. \square

Corollary 1.7 (of corollary 1.4). *For $p = 2, 3$ or 5 , $\#\mathcal{C}(\mathbf{Q}_p) \neq 0$.*

Proof. In this case, start with the solution $(3 : 1 : 1) \in \mathbf{P}^2(\mathbf{F}_p)$.

If $p = 2$ or 5 , take $G(T) = 3X^3 + 4 + 5$, and check that $|G(3)|_p < 1$ and $|G'(3)|_p = 1$.

If $p = 3$, we can lift the solution $(0 : 1 : 1) \in \mathcal{C}(\mathbf{F}_p)$ as follows. We just need to find a number $y \in \mathbf{Q}_3$ with $4y^3 + 5 = 0$. It is enough to solve $8y^3 + 10 = (2y)^3 + 10 = 0$, so it's enough to solve $v^3 + 10 = 0$. Make a change of variables $v = 3u - 1$:

$$(3u - 1)^3 + 10 = 27u^3 - 27u^2 + 9u + 9 = 9(3u^3 - 3u + u + 1).$$

So it's enough to solve $F(u) = 0$, where $F(u) = 3u^3 - 3u + u + 1$. Now check that $|F(2)|_3 = 3^{-1} < 1$ and $|F'(2)|_3 = |2|_3 = 1$, so Hensel's lemma applies. \square

1.2.1 Example

For the case $\mathcal{C} : 3X^3 + 4Y^3 + 5Z^3 = 0$, and for $p = 7$, we have $\mathcal{C}(\mathbf{F}_7) = \{(1 : 1 : 0)\}$. This point can be lifted (via the algorithm given in the proof of Hensel's lemma) to a point $(\alpha : 1 : 0)$, where

$$\alpha = 1 + 3 \cdot 7 + 3 \cdot 7^2 + 5 \cdot 7^4 + 5 \cdot 7^5 + 3 \cdot 7^6 + 5 \cdot 7^7 + \dots \in \mathbf{Q}_7,$$

with $3\alpha^3 + 4 = 0$. We can transform this curve into Weierstrass form:

$$\left. \begin{array}{l} X - \alpha Y = 0 \rightarrow Z = 0 \\ (\alpha : 1 : 0) \rightarrow (0 : 1 : 0) \end{array} \right\} \text{ is achieved by } \begin{cases} X' = Z \\ Y' = X + \alpha Y \\ Z' = X - \alpha Y \end{cases} \Rightarrow \begin{cases} \text{so } X = \frac{Y'+Z'}{2}, Y = \frac{Y'-Z'}{2\alpha}, Z = X'. \\ \text{On substitution, } \mathcal{C} \text{ becomes:} \\ 5X'^3 + \frac{9}{4}Z'Y'^2 + \frac{3}{4}Z'^3 = 0 \end{cases}$$

Scaling of coordinates by $X' = -x/5, Y' = y/15, Z' = 4z$ gives (in affine coordinates)

$$E : y^2 = x^3 - 1200.$$

Since $7 \nmid 1200$, the curve $E : y^2 = x^3 - 1200$, is smooth mod 7, so $E^0(\mathbf{Q}_7) = E(\mathbf{Q}_7)$. We have

$$E^0(\mathbf{Q}_7)/E^1(\mathbf{Q}_7) \cong E(\mathbf{F}_7) = \{(0 : 2 : 1), (0 : -2 : 1), (0 : 1 : 0)\}.$$

The nonzero (zero as in zero of group law, $(0 : 1 : 0)$) points lift to point $Q = (0 : \beta : 1)$ and $(0 : \beta : 1)$ with $\beta = \sqrt{1200} = 2 + 6 \cdot 7 + 5 \cdot 7^2 + 3 \cdot 7^3 + 7^4 + 6 \cdot 7^5 \dots \in E(\mathbf{Q}_7)$, which are points of order 3, and which map to the points $(\rho\alpha : 1 : 0)$ and $(\rho^2\alpha : 1 : 0)$ on the original curve, where $\rho^3 = 1, \rho \neq 1$.

We've previously seen that there are no other elements of finite order in $E(\mathbf{Q}_7)$. Recall that we have a filtration with elements such as $(7^n : \sqrt{1 - 7^{6n}1200} : 7^{3n}) \in E^n(\mathbf{Q}_7) \setminus E^{n+1}(\mathbf{Q}_7) \subset E(\mathbf{Q}_7)$.

In fact, it turns out (See Silverman VII §2 and IV §§1–3) that there is an isomorphism

$$\begin{aligned} 7\mathbf{Z}_7 &\rightarrow E^1(\mathbf{Q}_7) \\ u &\mapsto (x(u), y(u)), \end{aligned}$$

with inverse $(x, y) \mapsto x/y$. For example, 7 maps to the point $P = (7 : 1 : \gamma)$, where $\gamma = 7^3 + 4 \cdot 7^9 + 3 \cdot 7^{10} + 3 \cdot 7^{11} + 3 \cdot 7^{12} + 6 \cdot 7^{13} + 6 \cdot 7^{14} + 5 \cdot 7^{15} + \dots$ satisfies

$$1200\gamma^3 + \gamma - 7^3 = 0.$$

Note that this equation has two other solutions in \mathbf{Z}_7 , but only this one is in $7^3\mathbf{Z}_7$, which is necessary for P to be in $E^1(\mathbf{Q}_7)$. $E^1(\mathbf{Q}_7)$ is generated by P in the same sense that \mathbf{Z}_7 is generated by 1. I.e., we have infinite sums, for example,

$$(7 : \sqrt{1 - 7^6 1200} : 7^3) = P - 2 \cdot 7^6 P + 2 \cdot 7^7 P - 2 \cdot 7^8 P + 2 \cdot 7^9 P + 3 \cdot 7^{11} P + 7^{13} P - 3 \cdot 7^{14} P \dots$$

2 C has no points globally

The idea is to show that if \mathcal{C} did have points, another curve, given by

$$E : X^3 + Y^3 + 60Z^3 = 0$$

would have more than one point, but that E in fact only has one point.

2.1 Using a point on \mathcal{C} to construct a point on E

Theorem 2.1. For a, b, c positive integers, let \mathcal{C} and \mathcal{D} be two cubic curves given by:

$$\begin{aligned} \mathcal{C} : ax^3 + by^3 + c &= 0, \\ \mathcal{D} : x^3 + y^3 + abc &= 0. \end{aligned}$$

Then if $(u : v : w)$ is a point on \mathcal{C} , then there is a point $(x : y : z)$ on \mathcal{D} with $z \neq 0$.

sketch of proof. From $(u : v : w)$, construct two points P_1 and P_2 on $\mathcal{D}(\overline{\mathbf{Q}})$,

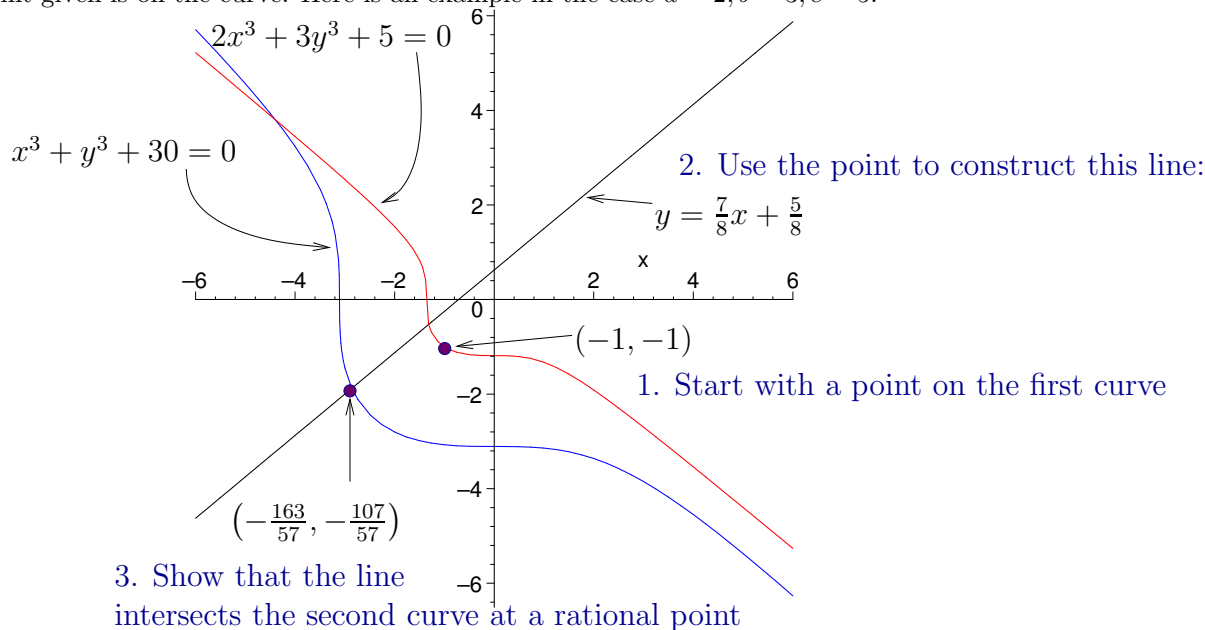
$$\begin{aligned} P_1 &= au^3 + \rho bv^3 + c\rho^2 w^3 \\ P_2 &= au^3 + \rho^2 bv^3 + c\rho w^3 \end{aligned}$$

which are conjugate under the action of the absolute Galois group of \mathbf{Q} . So the line through them must be defined over \mathbf{Q} . If $uv \neq 0$, for an appropriate choice of P_1, P_2 , this line is given by:

$$L : y = \left(\frac{au^3 - cw^3}{bv^3 - cw^3} \right) x + \left(\frac{au^3 - bv^3}{cw^3 - bv^3} \right) \frac{w^3}{uv}.$$

(Note, at most one of u, v, w can be zero, so we can always choose some pair of them with nonzero product, if $uv = 0$; everything else works in the same way.) Since L and \mathcal{D} are defined over \mathbf{Q} , the points in $L \cap \mathcal{D}$ are permuted by the Galois action. Since we know two are interchanged under nontrivial actions on the three points, the remaining point must be fixed, and so is defined over \mathbf{Q} . \square

Cassels gives more details of where this construction comes from (page 86), and a proof that the point given is on the curve. Here is an example in the case $a = 2, b = 3, c = 5$:



Corollary 2.2. If there is a point on $3x^3 + 4y^3 + 5z^3 = 0$, then there is a point on $x^3 + y^3 + 60z^3 = 0$ with nonzero z coordinate.

The next step is to show that $x^3 + y^3 + 60z^3 = 0$ has no points other than the zero at $(1 : -1 : 0)$. We do this in two parts: i) There are no points of finite order. ii) There are no points of infinite order.

Lemma 2.3. The curve $\mathcal{E} : x^3 + y^3 - 60$, has no points of finite order, other than the zero $(1 : -1 : 0)$.

Proof. In §6, Lemma 1, page 24, Cassels shows how this curve has no exceptional points other than $(1 : -1 : 0)$, by showing that when the tangent process is applied to a point $(x_1 : y_1 : z_1)$, with $z_1 \neq 0$, we get (x_2, y_2, z_2) , with $|z_2| > |z_1|$, where $\gcd(x_i, y_i, z_i) = 1$ for $i = 1, 2$. The tangent process sends P to $-2P$, so this process gives all points of the form $(-2)^n P$, all with different z coordinates, and so all distinct. If P had finite order, this would only be finitely many points, a contradiction. \square

Lemma 2.4. $E : X^3 + Y^3 + 60Z^3 = 0$, with zero at $(1 : -1 : 0)$, is isomorphic over \mathbf{Q} to

$$E' : y^2 = x^3 - 3^3 30^2.$$

Proof. The tangent line to E at $(1 : -1 : 0)$ is $X + Y = 0$. We want zero $(0 : 1 : 0)$, with tangent $Z = 0$.

$$\left. \begin{array}{l} X + Y = 0 \rightarrow Z = 0 \\ (1 : -1 : 0) \rightarrow (0 : 1 : 0) \end{array} \right\} \text{ is achieved by } \begin{cases} X' = Z \\ Y' = X - Y \\ Z' = X + Y \end{cases} \Rightarrow \begin{cases} \text{so } X = \frac{Y'+Z'}{2}, Y = \frac{Y'-Z'}{2}, Z = X'. \\ \text{On substitution, } E \text{ becomes:} \\ 4 \cdot 60X'^3 + 3Y'Z'^2 + Y'^3 = 0 \end{cases}$$

Appropriate scaling of y and z gives $y^2 = x^3 - 3^3 30^2$ \square

Lemma 2.5. For $E : y^2 = x^3 - 3^3 \cdot 30^2$, the group $E(\mathbf{Q})/2E(\mathbf{Q})$ is trivial.

Sketchy proof. Recall that in the proof of the Mordell theorem we defined a group homomorphism ϕ ,

$$\begin{aligned} \phi : E(\mathbf{Q}) &\longrightarrow \mathbf{Q}[\xi]/\mathbf{Q}[\xi]^2 \\ (a : b : 1) &\mapsto a - \xi \pmod{\mathbf{Q}[\xi]^2} \\ (0 : 1 : 0) &\mapsto 1 \pmod{\mathbf{Q}[\xi]^2}, \end{aligned}$$

where ξ , which (by an embedding) we take to be in \mathbf{R} , satisfies

$$\xi^3 - 3^3 \cdot 30^2 = 0.$$

We have $K := \mathbf{Q}[\xi] = \mathbf{Q}[\delta]$, where $\delta = \sqrt[3]{30}$. Note that $\xi = 3 \cdot 30/\delta = 3\delta^2$. The ring of integers is $\mathcal{O}_K = \mathbf{Z}[1, \delta, \delta^2]$, and fundamental unit $\mu = 1 + 9\delta - 3\delta^2$, with $1/\mu = 84\delta^2 + 261\delta + 811$. The group of units is given by $\langle -1, \mu \rangle$. In \mathcal{O}_K , for $p = 2, 3$ or 5 , the ideal (p) factors as $(p) = \mathfrak{p}_p^3$ where $\mathfrak{p}_p = (\delta, p)^3$. K has Galois closure $L = K[\rho]$, with ring of integers \mathcal{O}_L where $\rho^3 = 1, \rho \neq 1$.

1) $(a - \xi)\mathcal{O}_K$ is square as an ideal: A point on E not at $(0 : 1 : 0)$ has the form $(a, b) = (\frac{s}{t^3}, \frac{r}{t^2})$, where $r, s, t \in \mathbf{Z}$, and $\gcd(s, t) = \gcd(r, t) = 1$. To be on the curve means that

$$b^2 = a^3 - 3^3 \cdot \delta^6 = (a - 3\delta^2)(a - 3\rho\delta^2)(a - 3\rho^2\delta^2).$$

We have to multiply through by t^6 to get elements of \mathcal{O}_L . If a prime (ideal) divides the first factor, by considering linear combinations of the terms, the prime must divide 30, and by taking conjugates in \mathcal{O}_L , its conjugates must divide the second two factors. But prime divisors of 30 are self conjugate, and so then if \mathfrak{p}^n divides the first factor, \mathfrak{p}^{3n} divides the product, and hence divides s^2 , and so n is even. So the ideal generated by $(a - \xi)$ is a square. So $a - \xi$ is a square up to multiplication by $\pm\mu$, i.e., $a - \xi = b^2, \mu b^2, -b^2$, or $-\mu b^2$ for some $b \in \mathcal{O}_K$. However, since $x^3 - 3^3 30^2 = 0$ only has one real solution, ξ , and $x^3 - 3^3 30^2 < 0$ for $x < \xi$, for any point $(a, b) \in E(\mathbf{Q})$, we have $a > \xi$ so $a - \xi > 0$, and since $b \in \mathbf{Q}[\xi] \subset \mathbf{R}$, $b^2 > 0$, and also $\mu > 0$ so the only possibilities are $a - \xi = b^2$ or μb^2 .

2) $a - \xi$ is square, so ϕ maps everything to $1 \pmod{\mathbf{Q}[\xi]^2}$, and so $2E = E$: Cassels shows this is not possible by assuming that $t^2(a - \xi) = r - 3\delta t^2 = \mu\alpha^2$ for some $\alpha \in \mathcal{O}_K$, and then equating coefficients of $1, \delta, \delta^2$ to arrive at a contradiction. \square

Corollary 2.6. $E(\mathbf{Q})$ has no points of infinite order.

Proof. By the Mordell theorem, $E(\mathbf{Q})$ is finitely generated. If there is a point of infinite order, one of the generators of $E(\mathbf{Q})$, say P , must have infinite order, and $P \notin 2E(\mathbf{Q})$, contradicting Lemma 2.5. \square

Applying Lemma 2.3, Lemma 2.4, and Corollary 2.6 gives us:

Theorem 2.7. $\#E(\mathbf{Q}) = 1$

Theorem 2.8 (Selmer). The curve $\mathcal{C} : 3X^3 + 4Y^3 + 5Z^3 = 0$ has no rational points.

Proof. If it did, by Corollary 2.2 $\#E(\mathbf{Q}) \geq 2$, contradicting Theorem 2.7, $\#E'(\mathbf{Q}) = 1$. \square