GENERAL 2-DESCENT

FRANZ LEMMERMEYER

1. General 2-descent

We still have not proved the weak Mordell-Weil Theorem completely: so far we know that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite only for elliptic curves with at least one rational point of order 2.

Assume therefore that $E : y^2 = x^3 + ax + b$ is an elliptic curve, and that $f(x) = x^3 + ax + b \in \mathbb{Z}[x]$ is irreducible. Then $K = \mathbb{Q}[x]/(f)$ is a cubic extension of $\mathbb{Q}$, and you may think of this field as $K = \mathbb{Q}(\theta)$, where θ is a root of f.

Let $P = (x, y) \in E(K)$ be a K-rational point; we define the Weil map $\alpha : E(K) \longrightarrow K^\times/K^{\times\,2}$ by

$$\alpha(P) = \begin{cases} 1 \cdot K^{\times\,2} & \text{if } P = \mathcal{O}, \\ b \cdot K^{\times\,2} & \text{if } P = (\xi, 0), \\ (x-\theta)K^{\times\,2} & \text{otherwise.} \end{cases}$$

We know that α is a group homomorphism.

Now f has three roots θ_j $(j = 1, 2, 3)$, which means that we have three homomorphisms $\alpha_i : E(K_i) \longrightarrow K_i^\times/K_i^{\times\,2}$. If we want to make these three homomorphisms into one map we have to introduce the splitting field $K = K_1K_2K_3$ of f; then we can define

$$\alpha = (\alpha_1, \alpha_2, \alpha_3) : E(K) \longrightarrow K^\times/K^{\times\,2} \times K^\times/K^{\times\,2} \times K^\times/K^{\times\,2}.$$

As before we have $\alpha_1(P)\alpha_2(P)\alpha_3(P) = 1 \cdot K^{\times\,2}$, and we know that $\ker\alpha = 2E(K)$.

By restriction we get a homomorphism $\alpha : E(\mathbb{Q}) \longrightarrow (K^\times/K^{\times\,2})^3$ which maps (x, y) to $((x-\theta_1)K^{\times\,2}, (x-\theta_2)K^{\times\,2}, (x-\theta_3)K^{\times\,2})$.

A Little Cohomology. Here we finally can see some Galois cohomology in action. Our goal is to show that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite; one way of doing this is to show that $E(K)/2E(K)$ is finite, where K denotes the splitting field of f. That this is good enough follows from the following

Lemma 1. *The natural map $\gamma : E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow E(K)/2E(K)$ has finite kernel.*

Proof. Taking Galois cohomology of the exact sequence

$$0 \longrightarrow E[2] \longrightarrow E(K) \xrightarrow{\;2\;} 2E(K) \longrightarrow 0$$

and observing that $E[2]^G = 0$ if f is irreducible gives

$$0 \longrightarrow E(\mathbb{Q}) \xrightarrow{[2]} E(\mathbb{Q}) \cap 2E(K) \longrightarrow H^1(G, E[2]). \tag{1}$$

This provides us with an injection $\ker\gamma \hookrightarrow H^1(G, E[2])$. Since the last group is finite, we are done. □

Although this is all we need to prove the weak Mordell-Weil theorem in general, we will need a stronger statement later on.

Proposition 2. *If f is irreducible, then $H^1(G, E[2]) = 0$.*

Proof. If $(K : \mathbb{Q}) = 3$, then the orders of G and $E[2]$ are coprime; this implies $H^1(G, E[2]) = 0$.

In order to prove this in the case $(K : \mathbb{Q}) = 6$, let $G = \mathrm{Gal}\,(K/\mathbb{Q}) \simeq S_3$, and let g denote the normal subgroup of order 3. The inflation-restriction sequence

$$0 \longrightarrow H^1(G/g, A^g) \xrightarrow{\inf} H^1(G, A) \xrightarrow{\mathrm{res}} H^1(g, A)$$

applied to $A = E[2]$ gives

$$0 \longrightarrow H^1(G/g, E[2]^g) \xrightarrow{\inf} H^1(G, E[2]) \xrightarrow{\mathrm{res}} H^1(g, E[2]).$$

Now $(\#g, \#E[2]) = (3, 4) = 1$, hence $H^1(g, E[2]) = 0$. Also $E[2]^g = 0$ since the automorphisms of order 3 in G cyclically permute the points $(\theta_i, 0)$ of order 2. Thus $H^1(G/g, E[2]^g) = 0$ and this implies $H^1(G, E[2]) = 0$. □

This immediately implies

Corollary 3. *The homomorphism $\gamma : E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow E(K)/2E(K)$ is injective.*

Similarly we have

Corollary 4. *The homomorphism $\alpha : E(\mathbb{Q}) \longrightarrow (K^\times/K^{\times\,2})^3$ has kernel $2E(\mathbb{Q})$.*

Proof. Clearly $\ker\alpha = E(\mathbb{Q}) \cap 2E(k)$. The exact sequence (1) now shows that $E(\mathbb{Q}) \cap 2E(k) = 2E(\mathbb{Q})$. □

Cassels, in his book "Lectures on Elliptic Curves", gives an elementary proof involving calculations with the group law. His proof, however, uses the fact that $(K_1 : \mathbb{Q}) = 3$ in an essential way; the proof given here generalizes much more easily.

Weak Mordell-Weil. Let us now imitate our proof that im α is finite in the case where the θ_i were integers. Here's what we did: Consider the equation

$$y^2 = (x - \theta_1)(x - \theta_2)(x - \theta_3)$$

and write

$$\begin{aligned} (x - \theta_1) &= \mathfrak{d}_1\mathfrak{a}^2, \\ (x - \theta_2) &= \mathfrak{d}_2\mathfrak{b}^2, \\ (x - \theta_3) &= \mathfrak{d}_3\mathfrak{c}^2, \end{aligned} \tag{2}$$

where the $\mathfrak{d}_i$ are squarefree integral ideals, and where $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ are fractional ideals. Since $(y^2) = \mathfrak{d}_1\mathfrak{d}_2\mathfrak{d}_3(\mathfrak{abc})^2$, the ideal $\mathfrak{d}_1\mathfrak{d}_2\mathfrak{d}_3$ must be a square.

Now assume that $\mathfrak{p} \mid \mathfrak{d}_1$ and let $\mathfrak{p}^k$ be the exact power of $\mathfrak{p}$ dividing $x - \theta_1$. Since $\mathfrak{d}_1$ is squarefree, k must be an odd integer. If $k < 0$, then $\mathfrak{p}^k$ is also the exact power of $\mathfrak{p}$ dividing $x - \theta_2$ and $x - \theta_3$ since θ_2, θ_3 are algebraic integers; thus the exact power of $\mathfrak{p}$ dividing y^2 is $\mathfrak{p}^{3k}$, which is a contradiction since y^2 is a square and $3k$ is odd.

Thus $k > 0$, and hence $x \equiv \theta_1 \bmod \mathfrak{p}$. Since $\mathfrak{p}$ does not divide the denominator of x, the same is true for $\mathfrak{d}_2\mathfrak{b}^2 = (x - \theta_2)$ and $\mathfrak{d}_3\mathfrak{c}^2 = (x - \theta_3)$. Since k is odd and $\mathfrak{d}_1\mathfrak{d}_2\mathfrak{d}_3$ is an ideal square, we must have $\mathfrak{p} \mid \mathfrak{d}_2$ or $\mathfrak{p} \mid \mathfrak{d}_3$. But then, by the argument above, $x \equiv \theta_2 \bmod \mathfrak{p}$ or $x \equiv \theta_3 \bmod \mathfrak{p}$. This implies that $\theta_1 - \theta_2 \equiv 0 \bmod \mathfrak{p}$ or

$\theta_1 - \theta_3 \equiv 0 \bmod \mathfrak{p}$. Thus $\mathfrak{p} \mid (\theta_1 - \theta_2)(\theta_2 - \theta_3)(\theta_3 - \theta_1)$. The square of the number on the right hand side is the discriminant of f. Thus we have proved

Proposition 5. *There are only finitely many triples $(\mathfrak{d}_1, \mathfrak{d}_2, \mathfrak{d}_3)$ of squarefree integral ideals satisfying (2): any prime ideal $\mathfrak{p} \mid \mathfrak{d}_1\mathfrak{d}_2\mathfrak{d}_3$ divides $(\theta_1-\theta_2)(\theta_2-\theta_3)(\theta_3-\theta_1)$; in particular, $\mathfrak{p}^2 \mid \operatorname{disc} f$.*

Now let $\operatorname{Cl}(K) = \{c_1, \dots, c_h\}$ be the class group of K, and choose ideals $\mathfrak{c}_1 \in c_1$, $\dots$, $\mathfrak{c}_h \in c_h$. Since $\mathfrak{a} \sim \mathfrak{c}_s$ for some $\mathfrak{c}_s$, there is an $\alpha \in K^\times$ such that $\mathfrak{a} = \alpha\mathfrak{c}_s$, and we get $(x - \theta_1) = \alpha^2\mathfrak{d}_1\mathfrak{c}_s^2$. Thus the ideal $\mathfrak{d}_1\mathfrak{c}_s^2$ is principal, say $\mathfrak{d}_1\mathfrak{c}_s^2 = (\delta_1)$ for some $\delta_1 \in K^\times$. Note that we can choose δ_1 from a finite set since the number of ideals $\mathfrak{d}_1\mathfrak{c}_s^2$ is finite. Now $(x - \theta_1) = (\delta\alpha^2)$. Thus the two elements generating these ideals agree up to units, i.e. we have $x - \theta_1 = \varepsilon\delta_1\alpha^2$. Since the unit group E_K of K is finitely generated, the group E_K/E_K^2 is finite, hence there exist units $\varepsilon_1, \dots, \varepsilon_t$ such that every unit ε can be written as $\varepsilon = \varepsilon_i \cdot \upsilon^2$ for some unit υ. Replacing α by $\upsilon\alpha$ and δ_1 by $\varepsilon_i\delta_1$ (this increases the number of possibilities for δ_1, but their number is still finite) we get $x - \theta_1 = \delta_1\alpha^2$.

We have proved:

Proposition 6. *Let $P = (x, y) \in E(\mathbb{Q})$. There are finitely many algebraic integers $\delta_i \in \mathcal{O}_K$ with the property that $x - \theta_i = \delta_i\alpha^2$ for some $\alpha \in K^\times$. Since $\alpha_i(P) = (x - \theta_i)K^{\times 2} = \delta_i K^{\times 2}$, the image of α in $(K^\times/K^{\times 2})^3$ is finite. In particular, $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite for any elliptic curve defined over $\mathbb{Q}$.*

For the applications we have in mind it is useful to improve this result somewhat. Observe that $(\delta) = \mathfrak{d}\mathfrak{c}_s^2$ for some squarefree ideal $\mathfrak{d}$ such that $\mathfrak{p} \mid \mathfrak{d}$ only for prime ideals with $\mathfrak{p}^2 \operatorname{disc} f$.

Now assume that $\mathfrak{p} \mid \mathfrak{d}$. Taking the norm of the equation $x - \theta = \delta\alpha^2$ gives $y^2 = N(x - \theta) = \pm a^2 N\mathfrak{d}$ for some rational number a. This implies that $N\mathfrak{d}$ is a square, and this is only possible if one of the following holds:

- $N\mathfrak{p} = p^2$ is a square;
- $\mathfrak{d}$ is divisible by two different prime ideals $\mathfrak{p}, \mathfrak{p}'$ of norm p.

Thus the possible factorizations of (p) are $(p) = \mathfrak{p}\mathfrak{p}'\mathfrak{p}''$, $(p) = \mathfrak{p}\mathfrak{q}$, and $(p) = \mathfrak{p}\mathfrak{q}^2$.

In the first two cases p is unramified, hence $\mathfrak{p} \nmid \operatorname{disc} K$ for $K = \mathbb{Q}(\theta)$. Now $\operatorname{disc} f = i^2 \operatorname{disc} K$ for some integer i called the index of θ. Thus if $\mathfrak{p} \mid (\delta)$, then $\mathfrak{p}$ must be a prime ideal of norm p^2 and with $p \mid i$.

In the last case we have $\mathfrak{p}\mathfrak{p}' \mid (m - \theta e^2)$; thus $p \mid \mathfrak{p}^2\mathfrak{p}'^2 \mid (m - \theta e^2)$. But now $\xi = \frac{1}{p}(m^2 - 2me^2\theta + e^4\theta^2) \in \mathcal{O}_K$; the fact that $p \nmid e$ implies that $\xi \notin \mathbb{Z}[\theta]$, hence $p \mid i$. We have proved:

Proposition 7. *In the equations $x - \theta_i = \delta_i\alpha^2$ we have $(\delta) = \mathfrak{d}\mathfrak{a}^2$ for some squarefree integral ideal $\mathfrak{d}$ whose prime factors $\mathfrak{p}$ are not inert and not totally ramified, and which satisfy $p \mid \frac{\operatorname{disc} f}{\operatorname{disc} K}$.*

2. Application

Let us now apply this technique to complete the proof that there is no elliptic curve defined over $\mathbb{Q}$ with a rational point of order 11. We know that such curves are parametrized by the rational points on the elliptic curve $E : u^2 + u = v^3 - v^2$, and that the five rational torsion points on E correspond to cusps and do not represent elliptic curves with a rational point of order 11. In order to complete the proof we have to show that E has rank 0.

To this end, substitute $u = \frac{y}{8} - \frac{1}{2}$ and $v = \frac{x}{4}$; this gives the Weierstrass equation $E : y^2 = x^3 - 4x^2 + 16$. The field k generated by a root θ of $f(x) = x^3 - 4x^2 + 16$ has the following properties:

- discriminant disc $k = -44$;
- class number $h_k = 1$
- integral basis $\{1, \frac{1}{2}\theta, \frac{1}{4}\theta^2\}$;
- fundamental unit $\varepsilon = 1 - \frac{1}{2}\theta$;
- 2 is totally ramified: $2\mathcal{O}_k = \mathfrak{l}^3$;
- 11 is not totally ramified: $11\mathcal{O}_k = \mathfrak{p}^2\mathfrak{q}$.

Here's a `pari` session in which these invariants are computed; the right column gives comments and (partial) outputs:

```
f=x^3-4*x^2+16
nf=bnfinit(f);              % initialize; the semicolon hides output
nf.clgp                     % class group  [1, [], []]
nf.disc                     % discriminant -44
nf.zk                       % integral basis [1, 1/2*x, 1/4*x^2]
nf.fu                       % fundamental unit [1/2*x - 1]
idealfactor(nf,2)           % factorization  [2, [0, 1, 0]~, 3]
idealfactor(nf,11)          % [11, [1, 2, 0]~, 2], [11, [5, 2, 0]~, 1]
```

Now recall that $x - \theta = \delta\beta^2$; writing $x = m/e^2$ we find $x - \theta e^2 = \delta\alpha^2$ for $\alpha \in k$. Since disc $f = -2^8 \cdot 11$, we have $i = 2^3$; since 2 is totally ramified in k, we find $\mathfrak{d} = 1$. Since k has class number 1, this means that δ must be a unit, and we have to consider the equations $m - \theta e^2 = \pm\varepsilon\alpha^2$.

Recall that $\pi = \theta/2$ is integral; actually $N(\pi) = 2$, so $\mathfrak{l} = (\pi)$ and $(\theta) = (2\pi) = \mathfrak{l}^4$. Next, if θ is the real root of f, then $m - \theta e^2 > 0$: in fact, the product $(x - \theta_1)(x - \theta_2)(x - \theta_3) = y^2$ is positive, and so is the product $(x - \theta_2)(x - \theta_3)$ because these factors are complex conjugates of each other.

Note that $\pi \approx -0.839$, so $\varepsilon = 1 - \pi > 1$. Thus we are left with $m - \theta e^2 = \alpha^2$ and $m - \theta e^2 = \varepsilon\alpha^2$; the first one, of course, has the trivial point $m = 1, \alpha = e = 0$. It remains to show that the second equation is impossible. Now there are two cases:

(1) m is odd; then $\varepsilon\alpha^2 \equiv m - \theta e^2 \equiv 1 \bmod \pi^2$. Since there are exactly 4 residue classes modulo π^2, namely $0, 1, \pi, 1 + \pi$, we have $\alpha^2 \equiv 0, 1 \bmod \pi^2$. Since $\varepsilon \not\equiv 1 \bmod \pi^2$, this is a contradiction.

(2) m is even: then e must be odd, and the left hand side is divisible by π^4 exactly. Writing $\alpha = \pi^2\beta$ and cancelling the factor π^4 we get $-2/\pi^3 \equiv (1-\pi)\beta^2 \bmod \pi^2$. Now $-2/\pi^3 = \pi^2 - 2\pi + 1 \equiv 1 \bmod \pi^2$, and the resulting congruence $1 \equiv (1 - \pi)\beta^2 \bmod \pi^2$ does not have a solution.

This implies that $\operatorname{im} \alpha_1 = 1 \cdot K^{\times 2}$. Since the automorphisms of order 3 cyclically permute the roots θ_i, we must have $\operatorname{im} \alpha_i = 1K^{\times 2}$ for all i, and this shows that $\operatorname{im} \alpha = 1 \cdot K^{\times 2}$.

The proof given here is an adaption of the original proof of Billing and Mahler, with some help from an article of Bryden Cais.