1.16 26/07/09 - The Height Machine

Recall that last time we had described a general "descent" procedure (1.15.11) which can be used to prove that a group is finitely generated. For this, we needed the notion of "size" or "height" on the abelian group. The goal for today is today is to define a *height function* on the set of rational points of an elliptic curve over $\mathbb{Q}$, and check that it satisfies the required properties for 1.15.11. This would then reduce the proof of Mordell's Theorem (1.15.8) to the weaker 1.15.9. We follow the treatment in [2, §3.2-3.3].

The right notion of height on the set of rational points of an elliptic curve is a little more subtle than one might expect. One could hope that a naive notion, say the absolute value of the x-coordinate might work. However, a little experimentation (2.2.3) shows that this definition fails 1.15.11(c) (why?). Nonetheless, anyone who has experimented with rational points on elliptic curves (see, e.g., 2.1.9(b)) is that what blows up very quickly as you take multiples of points on an elliptic curve are the sizes of the numerators and denominators of the coordinates. The right definition of height, as it turns out, is indeed complexity-theoretic.

Definition 1.16.1.

(a) Let $q \in \mathbb{Q}$, and write q in lowest terms as $q = u/v$ for $u, v \in \mathbb{Z}$ with $v \geq 1$ and $\gcd(u, v) = 1$. Define the *height* $H(q)$ of q to be

$$H(q) := \max\{|u|, |v|\} \in \mathbb{Z}_{\geq 1},$$

and the *logarithmic height* $h(q)$ of q to be

$$h(q) := \log H(q) \in [0, \infty).$$

(b) Let $E/\mathbb{Q}$ be an elliptic curve in Weierstrass form. Given a point $P \in E(\mathbb{Q}) \setminus \{\mathscr{O}\}$, we define the *height* (resp. *logarithmic height*) of P by $H(P) := H(x(P))$ (resp. $h(P) := h(x(P)) = \log H(P)$). By convention, we also define $H(\mathscr{O}) = 1$ so that $h(\mathscr{O}) = 0$.

Observation 1.16.2. Given any $C_1 \in \mathbb{R}_{\geq 0}$, the set $\{q \in \mathbb{Q} : h(q) \leq C_1\}$ is finite.

Remark 1.16.3.

(a) Roughly speaking, the logarithmic height of a rational number is approximately the number of bits a computer might need to store it. I am also being deliberately vague about the base of the logarithm above–it doesn't really matter, as long as you pick one base and stick with it throughout.

(b) There is nothing really special about the function $u/v \mapsto \max\{|u|, |v|\}$; we could easily have chosen something different such as $u/v \mapsto |u| + |v|$ or $u/v \mapsto \sqrt{u^2 + v^2}$. This wouldn't give the same exact H or h, but the resulting H and h would be comparable thanks to

$$\frac{1}{2}(|u| + |v|) \leq \max\{|u|, |v|\} \leq |u| + |v| \text{ and } \frac{1}{\sqrt{2}}\sqrt{u^2 + v^2} \leq \max\{|u|, |v|\} \leq \sqrt{u^2 + v^2},$$

and we would get the same results (which you can later check!). It is sometimes advantageous to use these different kinds of heights instead; one such example of where the ℓ_2 height given by $u/v \mapsto \sqrt{u^2 + v^2}$ is more useful can be found in [16]. For another example of where the ℓ_1 height $u/v \mapsto |u| + |v|$ is more useful, see the proof of 1.16.6 (the part after 1.16.7).

(c) Similarly, there is nothing really special about taking the height of the x coordinate of a point, as opposed to that of its y-coordinate. See 1.16.4.

Lemma 1.16.4. Let $E/\mathbb{Q}$ be an elliptic curve in short Weierstrass form $y^2 = x^3 + ax^2 + bx + c$ with $a, b, c \in \mathbb{Z}$. There is an absolute constant $C_4 \in \mathbb{R}_{\geq 0}$ depending only on a, b, c with the following property: for any $P = (m/e^2, n/e^3) \in E(\mathbb{Q}) \setminus \{\mathscr{O}\}$ as in 1.14.8 with $m, n, e \in \mathbb{Z}$ and $e \geq 1$ and $\gcd(m, e) = \gcd(n, e) = 1$, we have that

$$|m| \leq H(P), \quad e^2 \leq H(P), \quad \text{and } |n| \leq C_4 \cdot H(P)^{3/2}.$$

In particular,

$$h(y(P)) \leq \frac{3}{2}h(P) + \log C_4. \tag{1.16.5}$$

Proof. The inequalities $|m| \leq H(P)$ and $e^2 \leq H(P)$ come from the definition of $H(P)$. To see the third one, note that by $P \in E(\mathbb{Q})$ we have the equality

$$n^2 = m^3 + am^2e^2 + bme^4 + ce^6.$$

Now using the triangle inequality and the first two inequalities, we see that

$$|n|^2 \leq |m|^3 + |a| \cdot |m|^2 \cdot e^2 + |b| \cdot |m| \cdot (e^2)^2 + |c| \cdot (e^2)^3 \leq (1 + |a| + |b| + |c|) \cdot H(P)^3,$$

so it suffices to take $C_4(E) := \sqrt{1 + |a| + |b| + |c|}$. The last inequality follows immediately upon taking logarithms. ∎

In fact, it is true that $h(y(P)) \asymp (3/2)h(P)$, i.e., there is also a constant making the inequality 1.16.5 go the other way. If you're curious, you can try to prove this; we won't need it, and so we won't prove it. We are now ready to prove what we wanted.

Theorem 1.16.6. Let $E/\mathbb{Q}$ be an elliptic curve in short Weierstrass form $y^2 = x^3 + ax^2 + bx + c$ with $a, b, c \in \mathbb{Z}$. The function

$$h : E(\mathbb{Q}) \to [0, \infty)$$

defined by 1.16.1(b) satisfies the conditions (a), (b), and (c) of 1.15.11. In other words, we have that:

(a) For each $C_1 \in \mathbb{R}_{\geq 0}$, the set $\{P \in E(\mathbb{Q}) : h(P) \leq C_1\}$ is finite.
(b) For each $Q \in E(\mathbb{Q})$, there is a $C_2(Q) \in \mathbb{R}_{\geq 0}$ such that for all $P \in E(\mathbb{Q})$, we have the inequality $h(P + Q) \leq 2h(P) + C_2(Q)$.
(c) There is a $C_3 \in \mathbb{R}_{\geq 0}$ such that for all $P \in E(\mathbb{Q})$, we have $h(2P) \geq 4h(P) - C_3$.

If you're still not too sure about where the general form of the conditions (a), (b), and (c) comes from, you will see the real source in the course of the following proof.

Proof. The condition (a) is automatic from 1.16.2 and the fact that each x-value corresponds to at most two y-values. Therefore, we have to show (b) and (c).

Let's show (b). If $Q = \mathscr{O}$, we can take $C_2(\mathscr{O}) = 0$. Hence suppose $Q \neq \mathscr{O}$. Note that it suffices to choose the $C_2(Q)$ such that the proposed inequality holds for all but finitely many P, say all except P_i, for we can always replace $C_2(Q)$ by the larger of $C_2(Q)$ and $\max_i\{2h(P_i) - h(P_i + Q)\}$. Therefore, it suffices to find a $C_2(Q)$ that works for all $P \in E(\mathbb{Q}) \setminus \{O, \pm Q\}$.

At this point, we just have to formula-crunch. Suppose that $Q = (x_0, y_0)$ and $P = (x, y)$. Since $P \neq \pm Q$, we have that $x \neq x_0$. Using the formulae in 1.12.D, we see that

$$x(P + Q) = \left(\frac{y - y_0}{x - x_0}\right)^2 - a - x - x_0 = \frac{(y - y_0)^2 - (x + x_0 + a)(x - x_0)^2}{(x - x_0)^2}.$$

Now the numerator contains a term of the form $y^2 - x^3$, which we can replace by $ax^2 + bx + c$, since $P \in E(\mathbb{Q})$. After clearing denominators of the rational coefficients, we see a general formula of the form

$$x(P + Q) = \frac{A_0y + A_1x^2 + A_2x + A_3}{A_4x^2 + A_5x + A_6}$$

for some $A_0, \ldots, A_6 \in \mathbb{Z}$ that depend only on a, b, c and Q but not on P. Next, we can use 1.14.8 to write P as $(m/e^2, n/e^3)$, where $m, n, e \in \mathbb{Z}$ and $e \geq 1$ with $\gcd(m, e) = \gcd(n, e) = 1$. This allows us to rewrite $x(P + Q)$ as

$$x(P + Q) = \frac{A_0ne + A_1m^2 + A_2me^2 + A_3e^4}{A_4m^2 + A_5me^2 + A_6e^4}.$$

This fraction may not be in its lowest terms, but we are only looking for an upper bound on the height, so we can certainly conclude that

$$H(P+Q) \leq \max\left\{|A_0ne + A_1m^2 + A_2me^2 + A_3e^4|, |A_4m^2 + A_5me^2 + A_6e^4|\right\}.$$

Again, the triangle inequality, along with the inequalities in 1.16.4, give us the estimates

$$|A_0ne + A_1m^2 + A_2me^2 + A_3e^4| \leq (|A_0C_4| + |A_1| + |A_2| + |A_3|) \cdot H(P)^2$$

and

$$|A_4m^2 + A_5me^2 + A_6e^4| \leq (|A_4| + |A_5| + |A_6|) \cdot H(P)^2,$$

so it suffices to take

$$C_2(Q) := \log\max\{|A_0C_4| + |A_1| + |A_2| + |A_3|, |A_4| + |A_5| + |A_6|\},$$

which again depends only on a, b, c and Q but not on P.

Finally, let's show (c). As in (b), we can ignore finitely many P_i, for we can always replace C_3 by the larger of C_3 and $\max_i\{4h(P_i) - h(2P_i)\}$. Therefore, it suffices to find a C_3 that works for all $P \in E(\mathbb{Q}) \smallsetminus E[2](\mathbb{Q})$. Again, at this point it is just formula-crunching, although there are some interesting ideas involved. Suppose that $P = (x, y)$. The duplication formula (1.12.12 and 1.14.3) tells us that the x-coordinate of $2P$ is

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4(x^3 + ax^2 + bx + c)}.$$

Let us write $x(P) = u/v$ in lowest terms, so that $u, v \in \mathbb{Z}$ with $v \geq 1$ and $\gcd(u, v) = 1$. (In the language of 1.14.8, we have $u = m$ and $v = e^2$.) Then the duplication formula looks like

$$x(2P) = \frac{u^4 - 2bu^2v^2 - 8cuv^3 + (b^2 - 4ac)v^4}{4(u^3v + au^2v^2 + buv^3 + cv^4)}.$$

For simplicity, let's call the numerator of this expression $\Phi(u, v)$, and the denominator $\Psi(u, v)$; both are integers, and we need to give an upper bound on their greatest common divisor. For this, we invoke

Lemma 1.16.7. Let $u, v \in \mathbb{Z}$ with $v \geq 1$ and $\gcd(u, v) = 1$. In the above notation,

$$\gcd(\Phi(u, v), \Psi(u, v)) \mid 4D,$$

where $D = \mathrm{disc}(f) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$ is as in 1.13.B.

Assuming this result for the moment, we finish the proof as follows: since we have bound the cancellation, we get a lower bound on the height of the form

$$H(2P) \geq \frac{1}{4D}\max\{|\Phi(u, v)|, |\Psi(u, v)|\} = \frac{v^4}{4D}\max\{|g(x)|, |4f(x)|\} \geq \frac{v^4}{4D} \cdot \frac{1}{2}\left(|g(x)| + |4f(x)|\right).$$

(This is where using the ℓ_1 height might have been a little easier.) We need to compare this with

$$H(P)^4 = \max\{u^4, v^4\} = v^4\max\{x^4, 1\}.$$

The ratio $H(2P)/H(P)^4$ cancels out the v^4 term (this is why there is 4 in (c)!), and we get that

$$\frac{H(2P)}{H(P)^4} \geq \frac{1}{8D}\frac{|g(x)| + |4f(x)|}{\max\{x^4, 1\}}.$$

Let's take a second to study the real function

$$\beta : \mathbb{R} \to [0, \infty), \quad x \mapsto \beta(x) := \frac{|g(x)| + |4f(x)|}{\max\{x^4, 1\}}.$$

Since $g(x)$ is a monic quartic polynomial and $f(x)$ is cubic, we have that

$$\lim_{x \to \pm 1}\beta(x) = 1.$$

Further, since $g(x)$ and $f(x)$ have no common roots (this uses nonsingularity of E, and was observed in the proof of 1.14.1), the function β never attains the value 0. These two facts, combined with the Extreme Value Theorem from calculus, are enough to conclude that β stays a positive distance away from the x-axis, i.e., that

$$\xi := \inf_{x \in \mathbb{R}} \beta(x) \in (0, \infty).$$

This gives us an inequality of the form

$$\frac{H(2P)}{H(P)^4} \geq \frac{\xi}{8D},$$

and so it suffices to take $C_3 := -\log(\xi/8D)$. To finish the proof of this theorem, it remains to give the

Proof of 1.16.7. Recall the polynomials

$$P(x) = 3x^3 - ax^2 - 5bx + 2ab - 27c \text{ and } Q(x) = -3x^2 - 2ax + a^2 - 4b$$

from the proof of 1.14.1, which had the property (1.14.4) that

$$P(x) \cdot 4f(x) + 4Q(x) \cdot g(x) = 4D.$$

Writing $x = u/v$ and multiplying throughout by v^7 gives us an equation of the form

$$\left(v^3 P\left(\frac{u}{v}\right)\right) \cdot \Psi(u, v) + v \cdot \left(v^2 Q\left(\frac{u}{v}\right)\right) \cdot \Phi(u, v) = 4Dv^7.$$

The quantities in parentheses are integers. Therefore, if we let $g := \gcd(\Phi(u, v), \Psi(u, v))$, then $g \mid 4Dv^7$. But since g also divides

$$\Phi(u, v) = u^4 - 2bu^2v^2 - 8cuv^3 + (b^2 - 4ac)v^4,$$

and $\gcd(u, v) = 1$, we conclude that $\gcd(g, v) = 1$. It follows from $g \mid 4Dv^7$ then that $g \mid 4D$. This finishes the proof of 1.16.7, ... ■

... and hence also of 1.16.6. ■

At this point, we have reduced the proof of Mordell's Theorem (1.15.8) to the 1.15.9. Next time, I will make a few more remarks about height before moving on to the proof of 1.15.9.