The Group of Rational Points

Alex Tao

14 July 2008

1 Heights and Descent

Let $x = \dfrac{m}{n}$ be a rational number, the height of x, $H(x)$ is defined as

$$H(x) = \max\{|m|, |n|\}.$$

The height, in some sense, measures the "complicatedness" of a rational number. If a rational number has a large height, then it means there is the need to go into very big numbers to construct the correct ratio for the number. It is easy to see that if $H(x)$ is some finite number, then the set of numbers with height less than $H(x)$ is a finite set. If $H(x)$ is less than some finite number, then both $|m|$ and $|n|$ is less than some finite number and there are only finitely many choices for m and n.

For some point P on the curve $y^2 = x^3 + ax^2 + bx + c$, the height of P is defined

$$H(P) = H(x).$$

Defining the "small h" function as

$$h(P) = \log H(P)$$

then $h(P)$ is always a non-negative real number. The finiteness property also translates to $h(P)$ as well as

$$\{P \in C(\mathbb{Q}) \ ; \ h(P) \leq M\}$$

being a finite set for some finite positive M since for every x there are only two possibilities for y on the curve. The height for the $\mathcal{O}$ is defined

$$H(\mathcal{O}) \quad \text{or} \quad h(\mathcal{O}).$$

To show that the group of rational points $C(\mathbb{Q})$ is generated by finitely many elements, we will need four lemmas. The first one has been proved above, but the rest will be proven later. For now, lets see how these four lemmas imply the result in the form of a theorem.

Descent theorem

Let Γ be a commutative group. Suppose that there is a function

$$h \ : \ \Gamma \longrightarrow [0, \infty)$$

with the following properties.
(a) For every real number M, the set $\{P \in \Gamma \ : \ h(P) \leq M\}$ is finite. (lemma 1)
(b) For every $P_0 \in \Gamma$, there is a constant κ_0 so that

$$h(P + P_0) \leq 2h(P) + \kappa_0 \qquad \text{for all } P \in \Gamma. \qquad \text{(lemma 2)}$$

(c) There is a constant κ so that

$$h(2P) \geq 4h(P) - \kappa \qquad \text{for all } P \in \Gamma. \qquad \text{(lemma 3)}$$

Suppose further that
(d) the subgroup 2Γ has finite index in Γ (lemma 4).
Then Γ is finitely generated.

Proof

Since 2Γ is a subgroup of Γ with finite index, there are only finitely many cosets of 2Γ in Γ. Let Q_1, Q_2,..., Q_n be the complete set of coset representatives. This means if we take an arbitrary element $P \in \Gamma$, there exists an index i_1 such that

$$P - Q_{i_1} \in 2\Gamma,$$

or specifically,

$$P - Q_{i_1} = 2P_1$$

for some $P_1 \in \Gamma$. Repeating the process on successive P_i ' s, we can write

$$\begin{aligned} P_1 - Q_{i_2} &= 2P_2 \\ P_2 - Q_{i_3} &= 2P_3 \\ &\vdots \\ P_{m_1} - Q_{i_m} &= 2P_m \end{aligned}$$

where Q_{i_1},Q_{i_2},..., Q_{i_m} are elements chosen from the coset representatives and P_1, P_2,...,P_m are some elements of Γ. Successive substitution for expressions of P_i's leads

$$\begin{aligned}
P &= Q_{i_1} + 2P_1 \\
P &= Q_{i_1} + 2Q_{i_2} + 4P_2 \\
&\vdots \\
P &= Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \cdots + 2^{m-1}Q_{i_m} + 2^m P_m
\end{aligned}$$

So every $P \in \Gamma$ can be represented this way by the finite set $\{Q_{i_1}, \ldots, Q_{i_m}\}$ and some P_m. The problem is we don't know if the P_m's in the expressions of every possible P is a finite set. Now, we will prove that if we choose a large enough m, then the height of P_m is always smaller than some constant and by (a), we know that the set of P_m's will be finite.

The first step is to use (b) and replace P_0 by $-Q_i$, we will find the constant κ_i from

$$h(P - Q_i) \leq 2h(P) + \kappa_i \qquad \text{for all } P \in \Gamma.$$

If we repeat this for each i (there are only finitely many by (d)) and find the largest of the κ_i's,κ', then the following holds

$$h(P - Q_i) \leq 2h(P) + \kappa' \qquad \text{for all } P \in \Gamma \text{ and all } 1 \leq i \leq n.$$

Combining (b) and (c) together and taking κ from (c), we can write the following inequalities

$$4h(P_j) \leq h(2P_j) + \kappa = h(P_{j-1} - Q_{i_j}) + \kappa \leq 2h(P_{j-1}) + \kappa' + \kappa.$$

Rewriting the result as

$$\begin{aligned}
h(P_j) &\leq \frac{1}{2}h(P_{j-1}) + \frac{\kappa' + \kappa}{4} \\
&= \frac{3}{4}h(P_{j-1}) - \frac{1}{4}\left(h(P_{j-1}) - (\kappa' + \kappa)\right).
\end{aligned}$$

We can see clear that if $h(P_{j-1}) \geq (\kappa' + \kappa)$, then

$$h(P_j) \leq \frac{3}{4}h(P_{j-1}).$$

If $h(P_m) \leq \kappa' + \kappa$, we are done since (a) tells us that the set of P_m's is a finite set. If $h(P_m) \geq \kappa' + \kappa$, we can use the relation $h(P_j) \leq \frac{3}{4}h(P_{j-1})$ we

can find $h(P_{m+i})$ for some $i > 0$ so that $h(P_{m+i}) \leq \kappa' + \kappa$, in particular, the set of $h(P_{m+i})$'s is a finite set.

If $P \in \Gamma$, then P can now be expressed as

$$P = a_1 Q_1 + a_2 Q_2 + \cdots + a_n Q_n + 2^m R$$

for certain integers $a_1, \ldots, a_n$ and some point $R \in \Gamma$ satisfying the inequality $h(R) \leq \kappa' + \kappa$. Since P is an arbitrary point in Γ, Γ is *finitely* generated by the elements in the union

$$\{Q_1, Q_2, \ldots, Q_n\} \cup \left\{R \in \Gamma : h(R) \leq \kappa' + \kappa\right\}$$

since (a) and (d) tells us these sets are finite.

□

This theorem brings the studies of elliptic curves, groups and number theory together and has involved the key idea of heights. The details of the proof, proving lemma 2,3 and 4 will be the topics of the next few sections.

2 The Height of $P + P_0$

It has been shown in the last chapter that for a rational point P in its lowest terms, $P = (\frac{m}{e}^2, \frac{n}{e}^3)$. From the definition of the height, $|m| \leq H(P)$ and $e^2 \leq H(P)$. Using the triangle inequality, we can induce a restriction on $|n|$.

Inserting the point P into the equation of curve and clearing the denominators by multiplying by e^6,

$$n^2 = m^3 + ae^2m^2 + be^4m + ce^6$$

using the triangle inequality

$$\begin{aligned} |n^2| &\leq |m^3| + |ae^2m^2| + |be^4m| + |ce^6| \\ &\leq H(P)^3 + |a|H(P)^3 + |b|H(P)^3 + |c|H(P)^3 \quad = H(P)^3(1 + |a| + |b| + |c|) \end{aligned}$$

Writing $K = \sqrt{1 + |a| + |b| + |c|}$, then we have

$$|n| \leq KH(P)^{\frac{3}{2}}.$$

Lemma 2

Let P_0 be a fixed rational point on C. There is a constant κ_0, depending on P_0 and on a, b, c, so that

$$h(P+P_0) \leq 2h(P) + \kappa_0 \quad \text{for all } P \in C(\mathbb{Q}).$$

Proof

If P is a point from the set $\{P_0, -P_0, \mathcal{O}\}$, then the result holds trivially. We will need to prove the result for an arbitrary number of P since a finite list will mean we can always choose a large enough κ_0 such that the result holds for the finite list. We will assume that P is any point on our curve with $P \notin \{P_0, -P_0, \mathcal{O}\}$.

Writing $P = (x, y)$ and $P_0 = (x_0, y_0)$ and working out the $P+P_0 = (\xi, \eta)$, the expression we find for η is

$$\xi = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G},$$

where A,B,C,D,E,F,G can be chosen to be integers that depend on a, b, c and (x_0, y_0). The point of this lemma is that chosen a fixed P_0, the results holds for *any* $P \notin \{P_0, -P_0, \mathcal{O}\}$ so κ_0 should not depend on x and y at all. Substituting $x = \frac{m}{e^2}$ and $y = \frac{n}{e^3}$ into the expresstion for ξ and clearing denomintors by e^4,

$$\xi = \frac{Ane + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4}.$$

If this fraction is not in its lowest term, the height of ξ will be smaller than the numerator and the denomintor, so in any case

$$H(\xi) \leq \max\{|Ane + Bm^2 + Cme^2 + De^4|, |Em^2 + Fme^2 + Ge^4|\}. \qquad (*)$$

Using the relations derived earlier,

$$e \leq H(P)^{\frac{1}{2}}, \qquad n \leq KH(P)^{\frac{3}{2}}, \qquad m \leq H(P),$$

and applying the triangle inequality on $(*)$, we find

$$H(P+P_0) = H(\xi) \leq \max\{|AK| + +|B| + |C| + |D|, |E| + |F| + |G|\}H(P)^2.$$

Taking the logarithm of both sides of the inequality and writing $\kappa_0 = \log\max\{|AK| + +|B| + |C| + |D|, |E| + |F| + |G|\}$, we have the result

$$h(P+P_0) \leq 2h(P) + \kappa_0.$$

So such κ_0 that does not depend on $P = (x, y)$ does exist.

$\square$

3 The Height of 2P

Here we need to show that the height of $2P$ is larger than 4 times of the height of P. It is convenient to use the duplication now to find out $x(2P)$ and work out its height. This proof will be harder than the previous one because we need to show a 'greater than' result and any cancellations in the fraction will lower the height and give us trouble.

Lemma 3

There is a constant κ, depending on a,b,c so that

$$h(2P) \geq 4h(P) - \kappa \quad \text{for all } P \in C(\mathbb{Q}).$$

Proof

Writing $P = (x, y)$ and $2P = (\xi, \eta)$ and starting off with the duplication formula, we have

$$\xi = \lambda^2 - a - 2x, \qquad \text{where } \lambda = \frac{f'(x)}{2y}$$

and so

$$\xi = \frac{(f'(x))^2 - (8x + 4a)f(x)}{4f(x)}.$$

We will ignore the case where $2P = \mathcal{O}$ since there are only finitely many of such P's and an appropriate κ can always be chosen. Also, from the assumption that the curve is non-singular, there are no common complex roots from $f(x)$ and $f'(x)$ and so we expect no common complex root in the numerator and denominator polynomial of ξ. Here, the degrees of the numerator and the denominator are 4 and 3 respectively.

In the slight change of notations, we are trying to prove

$$h(\xi) \geq 4h(x) - \kappa.$$

We can translate this lemma into a general result in heights and polynomials without considering any curves.

Lemma 3′

Let $\phi(X)$ and $\psi(X)$ be polynomials with integer coefficients and no common (complex) roots. Let d be the maximum of the degrees of ϕ and ψ.
(a) There is an integer $R \geq 1$, depending on ϕ and ψ, so that for all rational numbers $\dfrac{m}{n}$,

$$\gcd\left(n^d\phi\left(\frac{m}{n}\right), n^d\psi\left(\frac{m}{n}\right)\right) \quad \text{divides } R.$$

(b) There are constants κ_1 and κ_2, depending on ϕ and ψ, so that for all rational numbers $\dfrac{m}{n}$ which are not roots of ψ,

$$dh\left(\frac{m}{n}\right) - \kappa_1 \leq h\left(\frac{\phi(m/n)}{\psi(m/n)}\right) \leq dh\left(\frac{m}{n}\right) + \kappa_2.$$

Proof

(a) This proof involves a lot of looking at which quantity divides which quantity and then finally designing a constant that can be divided by $\gcd\left(n^d\phi\left(\frac{m}{n}\right), n^d\psi\left(\frac{m}{n}\right)\right)$. The point of this part is to fix a bound on the cancellation of the fraction and subsequently fixing a lower bound on the height. We first write

$$\Phi(m,n) = n^d\phi = a_0m^d + a_1m^{d-1}n + \cdots + a_dn^d,$$
$$\Psi(m,n) = n^d\psi = b_0m^en^{d-e} + b_1m^{e-1}n^{d-e+1} + \cdots + b_en^d$$

Since $\phi(X)$ and $\psi(X)$ have no common roots, they have no common components and so are coprime to each other. By Bezout, this means there exists $F(X)$ and $G(X)$ such that

$$F(X)\phi(X) + G(X)\psi(X) = 1. \qquad (*)$$

We can introduce an A so that $AF(X)$ and $AG(X)$ has integer coordinates and a D to be the maximum degree of $F(X)$ and $G(X)$. If we put $X = \dfrac{m}{n}$ and multiply $(*)$ through by An^{D+d}, we have

$$n^DAF\left(\frac{m}{n}\right)\cdot\Phi(m,n) + n^DAG\left(\frac{m}{n}\right)\cdot\Psi(m,n) = An^{D+d}.$$

The multipliers of $\Phi(m,n)$ and $\Psi(m,n)$ in the above equation are integer quantities so if we define $\gamma(m,n) := \gcd(\Phi(X),\Psi(X))$, we can see that γ divides An^{D+d}.

Observe that the LHS of the equation

$$An^{D+d-1}\Phi(m,n) = Aa_0m^dn^{D+d-1} + Aa_1m^{d-1}n^{D+d} + \cdots + Aa_dn^{D+2d-1}$$

can be divided by γ because $\gamma|\Phi$. On the right hand side, each term except from the first term contains An^{D+d} which is divisible by γ. It follows that γ divides the term $Aa_0m^dn^{D+d-1}$. We now know that γ divides the $\gcd(An^{D+d}, Aa_0m^dn^{D+d-1})$, but since m and n are coprime, we can conclude that $\gamma|Aa_0n^{D+d-1}$. Repeating this procedure, we keep reducing the power of n and increasing the power of a_0, eventually we will find that γ divides Aa_0^{D+d}. This completes the proof of (a).
(b) The upper bound can be proved by similar methods as the proof of lemma 2 so we will only consider the lower bound here.

$$H(\xi) = \max \Phi(m,n), \Psi(m,n)$$

Using the result from part (a), there is a maximum bound to the common factor of the numerator and denominator so we can write

$$\begin{aligned} H(\xi) &\geq \frac{1}{R}\max\{|\Phi(x)|, |\Psi(x)|\} \\ &\geq \frac{1}{2R}\left(|\Phi(x)| + |\Psi(x)|\right) \end{aligned}$$

Now the key step is to take the ratio of $H\left(\frac{m}{n}\right)^d$ with the above,

$$\begin{aligned} \frac{H(\xi)}{H(m/n)^d} &\geq \frac{1}{2R}\cdot\frac{\left(\left|n^d\phi\left(\frac{m}{n}\right)\right| + \left|n^d\psi\left(\frac{m}{n}\right)\right|\right)}{\max\{|m|^d, |n|^d\}} \\ &= \frac{1}{2R}\cdot\frac{\left(\left|\phi\left(\frac{m}{n}\right)\right| + \left|\psi\left(\frac{m}{n}\right)\right|\right)}{\max\left\{\left|\frac{m}{n}\right|^d, 1\right\}}. \end{aligned}$$

We can consider a real continuous function

$$p(t) = \frac{|\phi(t)| + |\psi(t)|}{\max\{|t|^d, 1\}}.$$

We can see this function is strictly positive afor all t. Firstly because of the modulus signs, it can never be negative. Secondly it cannot be zero as we assumed the $\phi(x)$ and $\psi(x)$ ahev no common roots, furthermore, we have a non-zero limit as t approaches infinity because the at least one of the polynomials in the numerator has degree d and limit will tend to either $|a_0|$ or $|a_0 + b_0|$ from the leading coefficients. This means for all real t there is an equality $p(t) \geq C_1$ for some $C_1 > 0$.

Rewriting our inequality for $H(\xi)$ using the above fact, we have

$$H(\xi) \geq \frac{C_1}{2R} H \left(\frac{m}{n}\right)^d,$$

or if we take logarithms,

$$h(\xi) \geq dh \left(\frac{m}{n}\right) - \kappa_1.$$

where $\kappa_1 = log(2R/C_1)$ and is independent of m and n. This completes the proof of lemma $3'$. For lemma 3, we know that the degree $d = 4$ so we have

$$h(\xi) \geq 4h \left(\frac{m}{n}\right) - \kappa_1.$$

$\square$