LECTURE 21, MONDAY 25.04.04

FRANZ LEMMERMEYER

1. Heights

Now we introduce the notion of heights of rational numbers and rational points on curves; heights are an important ingredient in the classical descent proofs. Eventually, heights will allow us to complete the proof of the Mordell-Weil theorem.

In many introductory texts the theory of heights is treated as a collection of dirty tricks. I hope that the exposition below convinces you that this is not true at all.

Heights of Rational Numbers. Heights measure how complicated rational numbers are. The absolute value is not useful for this purpose since it assigns the numbers $x = 1$ and $x = \frac{10000}{9999}$ similar absolute values, although the second one is much more complicated.

This suggests the definition $H(x) = \max\{|p|, |q|\}$ for $x = \frac{p}{q}$ with $\gcd(p, q) = 1$.

In fact, this agrees with our notion of 'small' in the proof of Fermat's last theorem, where the size of integral solutions (x, y, z) of $x^4 + y^4 = z^2$ was measured by $|z|$: observe that $(x/y, z/y^2)$ is a rational point on $u^4 + 1 = v^2$, and that $H(v) = |z|$ since $y^2 < |z|$.

The height function has a few almost trivial properties:

Lemma 1. *For $x, y \in \mathbb{Q}^\times$ we have*

1. $H(xy) \le H(x)H(y)$;
2. $H(x^n) = H(x)^n$ *for all* $n \in \mathbb{Z}$;
3. $H(x + y) \le 2H(x)H(y)$;
4. *the number of rational numbers with bounded height is finite: for every* $c > 0$ *we have* $\#\{x \in \mathbb{Q} : H(x) \le c\} < \infty$.

Proof. Write $x = \frac{r}{s}$ and $y = \frac{t}{u}$. Then $xy = \frac{rt}{su}$ and $H(xy) \le \max\{|rt|, |su|\}$. Note that $|r|, |s| \le H(x)$ and $|t|, |u| \le H(y)$, hence $H(xy) \le H(x)H(y)$. Observe that we don't always have equality in 1, as the example $x = \frac{1}{y}$ shows.

The second property follows from unique factorization: if $x = \frac{r}{s}$ with $\gcd(r, s) = 1$, then $x^n = \frac{r^n}{s^n}$ with $\gcd(r^n, s^n) = 1$.

Next $x + y = \frac{ru+st}{su}$, hence $H(xy) \le \max\{|ru + st|, |su|\}$, and $|ru + st| \le |ru| + |st| \le 2H(x)H(y)$ as well as $|su| \le H(x)H(y)$.

The last property is again clear, since there are only finitely many rational numbers whose numerator and denominator are bounded by c. □

It will be important for us to know how the height behaves under rational maps. For simple maps like $f(x) = x^n$, we have seen that $H(f(x)) = H(x)^n$. More generally, if $f \in \mathbb{Z}[X]$ is a polynomial of degree n, then $H(f(x))/H(x)^n$ can easily be bounded from above:

Lemma 2. *If $f(X) = a_nX^n + \ldots + a_1X + a_0 \in \mathbb{Z}[X]$, then*

$$H(f(x)) \le (n+1)MH(x)^n$$

for all $x \in \mathbb{Q}$, where $M = \max\{|a_0|, |a_1|, \ldots, |a_n|\}$.

Proof. Write $x = \frac{p}{q}$ with $\gcd(p,q) = 1$; then $H(x) = \max\{|p|, |q|\}$, and in particular we have $|p| \le H(x)$ and $|q| \le H(x)$. Now

$$\begin{aligned} |q^n f(x)| &= |a_np^n + a_{n-1}p^{n-1}q + \ldots + a_1q^{n-1}p + a_0q^n| \\ &\le |a_n||p|^n + |a_{n-1}||p|^{n-1}|q| + \ldots + |a_1||p||q|^{n-1} + |a_0||q|^n \\ &\le (n+1)mH(x)^n, \end{aligned}$$

because $|a_k| \le M$ and $|p|^r|q|^{n-r} \le H(x)^rH(x)^{n-r} = H(x)^n$. □

Finding a lower bound for the height of $f(x)$ is just as easy: consider

$$f(x) = \frac{a_np^n + a_{n-1}p^{n-1}q + \ldots + a_1q^{n-1}p + a_0q^n}{q^n};$$

then the greatest common divisor of q and the numerator divides a_n, therefore the gcd of q^n and the numerator divides a_n^n. Thus there cannot be too much cancellation, and we find $H(f(x)) \ge |a_n|^{-n}q^n \ge |a_n|^{-n}H(x)^n$.

We have proved:

Lemma 3. *If $f(X) = a_nX^n + \ldots + a_1X + a_0 \in \mathbb{Z}[X]$, then*

$$H(f(x)) \ge |a_n|^{-n}H(x)^n.$$

Thus we have proved that there exist constants $c_1, c_2 > 0$ depending only on f (and not on x) such that

$$c_1H(x)^n \le H(f(x)) \le c_2H(x)^n.$$

This result will now be generalized from polynomials to rational functions.

Consider polynomials $f(x) = a_nx^n + \ldots + a_1x + a_0 \in \mathbb{Z}[x]$ and $g(x) = b_mx^m + \ldots + b_1x + b_0 \in \mathbb{Z}[X]$, and assume without loss of generality that $n \ge n$. Then

$$\frac{f(x)}{g(x)} = \frac{F(p,q)}{G(p,q)},$$

where F is the homogenization of f, and where G is q^{n-m} times the homogenization of g. Note that $\deg F = \deg G = n$.

Now $H(f(x)/g(x))$ is bounded above by the heights of $F(p,q)$ and $G(p,q)$, hence we have

$$H\Big(\frac{f(x)}{g(x)}\Big) \le (n+1)MH(x)^n,$$

where $M = \max\{M_f, M_g\}$, and M_f and M_g are the constants coming from the application of Lemma 3.

In order to find a lower bound for the height, observe that

$$H\Big(\frac{f(x)}{g(x)}\Big) = H\Big(\frac{P}{Q}\Big) = \frac{\max\{|P|, |Q|\}}{\gcd(P,Q)},$$

where $P = F(p,q)$ and $Q = G(p,q)$, so we need a lower bound for $\max\{|P|, |Q|\}$ and an upper bound for $\gcd(P,Q)$ at the same time.

Now let f_1 and g_1 denote the dehomogenizations of F and G with respect to X, and let $R = \operatorname{res}(f_1, g_1)$ denote the resultant of f_1 and g_1. Then there exist

polynomials $u_1, v_1 \in \mathbb{Z}[x]$ with $\deg u_1 < \deg g_1 = n$ and $\deg v_1 < \deg f_1 = n$ such that $f_1 u_1 + g_1 v_1 = R$. Homogenizing gives the equation

$$F(X,Y)U_1(X,Y) + G(X,Y)V_1(X,Y) = RX^{2n-1}. \tag{1}$$

Dehomogenizing with respect to Y and repeating this process similarly gives polynomials u_2, v_2 with homogenizations U_2, V_2 such that

$$F(X,Y)U_2(X,Y) + G(X,Y)V_2(X,Y) = RY^{2n-1}. \tag{2}$$

Plugging in $X = p$ and $Y = q$ shows that

$$\gcd(F(p,q), G(p,q)) \mid Rp^{2n-1}, \quad \text{and} \quad \gcd(F(p,q), G(p,q)) \mid Rq^{2n+1}.$$

Since $\gcd(p,q) = 1$, we deduce that $\gcd(F(p,q), G(p,q)) \mid R$.

On the other hand, setting $X = p$ and $Y = q$ in equation (1) shows that

$$|q|^{2n-1}|R| \leq |F(p,q)U_1(p,q)| + |G(p,q)V_1(p,q)|.$$

Now $|U_1(p,q)| \leq C_1 H(x)^{n_1}$ and $|V_1(p,q)| \leq C_2 H(x)^{n-1}$, hence

$$|q|^{2n-1}|R| \leq CH(x)^{n-1} \cdot \max\{|F(p,q)|, G(p,q)|\}.$$

This implies

$$\max\{|F(p,q)|, G(p,q)|\} \geq |q|^{2n-1}|R|c_1 H(x)^{1-n}.$$

Repeating this argument with equation (2), we similarly get

$$\max\{|F(p,q)|, G(p,q)|\} \geq |p|^{2n-1}|R|c_2 H(x)^{1-n}.$$

Thus

$$\max\{|F(p,q)|, G(p,q)|\} \geq c|R| \cdot (\max\{|p|, |q|\})^{2n-1} H(x)^{1-n} = c|R| \cdot H(x)^n,$$

and this finally implies

$$H\Big(\frac{f(x)}{g(x)}\Big) = \frac{\max\{|P|, |Q|\}}{\gcd(P,Q)} \geq c \cdot H(x)^n.$$

We have proved:

Proposition 4. *Let $f, g \in \mathbb{Z}[X]$ be coprime, and put $n = \max\{\deg f, \deg g\}$. Then there exist constants $C_1, C_2 > 0$ such that for all $x \in \mathbb{Q}$ we have*

$$C_1 H(x)^n \leq H\Big(\frac{f(x)}{g(x)}\Big) \leq C_2 H(x)^n.$$