SIEGEL'S THEOREM

VIVIAN KUPERBERG

1. Notation Used Throughout

K a number field;
E/K an elliptic curve over K;
M_K a complete set of inequivalent absolute values on K;
M_K^∞ (resp. M_K^0) the archimedean (resp nonarchimedean) absolute values on M_K;
$v(x) = -\log|x|_v$ for $v \in M_K$, $|\cdot|_v$ the normalized absolute value for $v \in M_K$;
R ring of integers of K, $R^\times$ unit group of R;
K_v completion of K at $v \in M_K$, R_v ring of integers of K_v;
H_K the projective height, $H_K(P) = \prod_{v\in M_K} \max_i\{|x_i|_v\}$ for $P = [x_0, \dots, x_N] \in \mathbb{P}^N(K)$;
$h_f = \log H_K(f(P))$ for $f : E \to \mathbb{P}^N$ the height on E
n_v is the local degree $[K_v : \mathbb{Q}_v]$
$\mathrm{ord}_Q(f)$ is the vanishing order of a function f at a point Q

2. Motivation and a classical question

The question that this talk is answering is generally "How many integral points are there on elliptic curves?" The answer (spoiler alert!) is generally "finitely many."

Remark 2.1. But wait! I hear you cry. I have an objection! We've already seen that there are infinitely many *rational* points on an elliptic curve. If it's a projective curve, then we can automatically say that there are infinitely many integer points, by just multiplying out the denominators.

Indeed we could! We will not be in the projective setting for this talk. We are in the affine setting.

Consider the following more specific and more classical question, which will help us on our way.

Question 2.2. Given an irrational number $x \in \mathbb{R}$, can we approximate x by a rational number $\frac{p}{q}$ where $\left|x - \frac{p}{q}\right|$ is small relative to q?

This question was posed by Dirichlet, who also gave the following answer.

Proposition 2.3 (Dirichlet). *Let $x \in \mathbb{R}$ be irrational. There are infinitely many $\frac{p}{q} \in \mathbb{Q}$ with*

$$\left|\frac{p}{q} - x\right| \leq \frac{1}{q^2}.$$

Most of the results in this talk are going to be about cases where we can't do this, i.e. a statement of the form *"There are only finitely many rational approximations of an irrational point where the error is small."* Here's the first one.

Proposition 2.4 (Liouville). *Let $\alpha \in \bar{\mathbb{Q}}$ with $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$ for $d \geq 2$. There exists a constant $C > 0$, dependent on α, such that for all $p/q \in \mathbb{Q}$ we have*

$$\left| \frac{p}{q} - \alpha \right| \geq \frac{C}{q^d}.$$

Here's an equivalent phrasing of Liouville's theorem which will motivate a definition to follow.

Proposition 2.5 (Liouville, again). *Let $\alpha \in \bar{\mathbb{Q}}$ with $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$ for $d \geq 2$. Fix any $\varepsilon > 0$ and any $C > 0$. There are only finitely many $\frac{p}{q} \in \mathbb{Q}$ with*

$$\left| \frac{p}{q} - \alpha \right| < C q^{-(d+\varepsilon)}.$$

This gives us the idea of an *approximation exponent* which is basically an option for something in the exponent of q. More generally:

Definition 2.6. Let K be a number field, and let $\tau(d) : \mathbb{N} \to \mathbb{R}_{>0}$. We say that τ is an *approximation exponent* for K if for any $\alpha \in \bar{K}$ with $[K(\alpha) : K] = d$ and for any $v \in M_K$ an absolute value on K extended to $K(\alpha)$, for any C there are only finitely many $x \in K$ with

$$|x - \alpha|_v < C H_K(x)^{-\tau(d)}.$$

So our third and most compact formulation of Liouville's theorem is that for all $\varepsilon > 0$, $\tau(d) = d + \varepsilon$ is an approximation exponent for $\mathbb{Q}$. Several incremental improvements were made on Liouville's result, culminating in Roth's theorem of 1955.

Theorem 2.7 (Roth). *For every $\varepsilon > 0$ and every number field K, $\tau(d) = 2 + \varepsilon$ is an approximation estimate.*

Remark 2.8. Another formulation of Dirichlet's theorem above is that 2 is *not* an approximation estimate for $\mathbb{Q}$, so in that sense this is the best we can do.

The proof of Roth's theorem has many steps, none of which are "tremendously deep," but it ends up being quite lengthy in full detail. See Silverman [2] for an outline. We will, however, discuss the following example in elliptic curves, which shows why this story becomes relevant.

Example 2.9. Consider the curve $x^3 - 2y^3 = k$, for $k \in \mathbb{Z}$. If $y \neq 0$, we can factor to get

$$\left(\frac{x}{y} - \sqrt[3]{2} \right) \left(\frac{x}{y} - \zeta \sqrt[3]{2} \right) \left(\frac{x}{y} - \zeta^2 \sqrt[3]{2} \right) = \frac{k}{y^3},$$

where ζ is a primitive third root of unity. The second and third factors are bounded away from 0 when x, y are integral, and this bounding is independent of the values of x and y. Thus there exists a constant C independent of x, y with

$$\left| \frac{x}{y} - \sqrt[3]{2} \right| \leq \frac{C}{|y|^3}.$$

By Roth's theorem, there can only be finitely many possibilities for x, y. Thus there are only finitely many integral points on this elliptic curve.

3. Distance Functions

In order to state Siegel's theorem, we'll need to briefly discuss distance functions.

Definition 3.1. Let C/K be a curve, let $v \in M_K$, and fix a point $Q \in C(K_v)$. Choose a function $t_Q \in K_v(C)$ with a zero of order $e \geq 1$ at Q and no other zeroes. Then for $P \in C(K_v)$, we define the *(v-adic) distance from P to Q* by

$$d_v(P,Q) = \min\left\{|t_Q(P)|_v^{1/e}, 1\right\}.$$

Remark 3.2. Such a t_Q must exist because of Riemann-Roch. If t_Q has a pole at P, we formally set $|t_Q(P)| = \infty$.

The mantra of distance functions is that "they're nicer than they appear." In fact, as defined, we have $d_v(P,Q)$ dependent on our choice of $t_Q(P)$, which seems bad. But, the following proposition shows that things are nicer than they appear; the choice of t_Q is irrelevant for our theorems.

Proposition 3.3. *For $Q \in C(K_v)$ and $F \in K_v(C)$ a function vanishing at Q, the limit*

$$\lim_{P \in C(K_v), P \to_v Q} \frac{\log |F(P)|_v}{\log d_v(P,Q)} = \operatorname{ord}_Q(F)$$

exists and is independent of the choice of t_Q.

Proof sketch. The clever step is noting that $\phi = \frac{F^{\operatorname{ord}_Q(t_Q)}}{t_Q^{\operatorname{ord}_Q(F)}}$ has neither a zero nor a pole at Q; writing the limit in terms of ϕ gives the result. □

The following is another computational fact about distance functions which we'll need but won't prove.

Proposition 3.4. *Let $\phi : C_1 \to C_2$ be a finite map defined over K of curves C_i/K. Let $Q \in C_1(K_v)$ and let $e_\phi(Q)$ be the ramification index of ϕ at Q. Then*

$$\lim_{P \in C_1(K_v) P \to_v Q} \frac{\log d_v(\phi(P), \phi(Q))}{\log d_v(P,Q)} = e_\phi(Q).$$

We will end our foray into distance functions with a reinterpretation of Roth's theorem in this language.

Corollary 3.5 (Roth's Theorem). *Fix $v \in M_K$. Let C/K be a curve, let $f \in K(C)$ be a nonconstant function, and let $Q \in C(\bar{K})$. Then*

$$\liminf_{P \in C(K), P \to_v Q} \frac{\log d_v(P,Q)}{\log H_K(f(P))} \geq -2.$$

Proof. Assume without loss of generality that $f(Q) \neq \infty$ (if not, replace f by $1/f$, which does not change $H_K(f(P))$. Let e be the order of the vanishing of $f - f(Q)$ at Q. Then by

Proposition 3.3,

$$\begin{aligned}\liminf_{P\in C(K),P\to_v Q} \frac{\log|f(P)-f(Q)|_v}{\log d_v(P,Q)} &= e\\ \Rightarrow \liminf_{P\in C(K),P\to_v Q} \frac{\log d_v(P,Q)}{\log H_K(f(P))} &= \liminf_{P\in C(K),P\to_v Q} \frac{\log|f(P)-f(Q)|_v}{e\log H_K(f(P))}\\ &= \frac{1}{e}\liminf\left(\frac{\log\left(H_K(f(P))^\tau |f(P)-f(Q)|_v\right)}{\log H_K(f(P))} - \tau\right).\end{aligned}$$

Setting $\tau = 2+\varepsilon$ for arbitrary $\varepsilon > 0$, Roth's theorem implies that

$$H_K(f(P))^\tau |f(P)-f(Q)|_v \geq 1$$

for almost all $P \in C(K)$. Thus

$$\liminf \frac{\log d_v(P,Q)}{\log H_K(f(P))} \geq -\frac{\tau}{e} \geq -\frac{2+\varepsilon}{e},$$

but $e \geq 1$ and ε is arbitrary, so this is the desired result. □

4. Siegel's Theorem

We'll now jump in with a statement of Siegel's Theorem, discuss the proof, and then talk about some consequences.

Theorem 4.1 (Siegel)**.** *Let E/K be an elliptic curve with $|E(K)| = \infty$. Fix a point $Q \in E(\bar{K})$, a nonconstant even function $f \in K(E)$, and an absolute value $v \in M_{K(Q)}$. Then*

$$\lim_{P\in E(K)h_f(P)\to\infty} \frac{\log d_v(P,Q)}{h_f(P)} = 0.$$

Remark 4.2. We'll prove this when f is even, but f doesn't have to be even.

Proof. Since $d_v(P,Q) \leq 1$ and $h_f(P) \geq 0$ for all points $P \in E(K)$, we have

$$\limsup_{P\in E(K)h_f(P)\to\infty} \frac{\log d_v(P,Q)}{h_f(P)} \leq 0.$$

We will prove that the lim inf is greater than or equal to 0, which suffices.

Let $P_i \in E(K)$ be a sequence of distinct points P_i with

$$\lim_{i\to\infty} \frac{\log d_v(P_i,Q)}{h_f(P_i)} = L = \liminf_{P\in E(K)h_f(P)\to\infty} \frac{\log d_v(P,Q)}{h_f(P)}.$$

Let $m \in \mathbb{N}$. We'll ultimately be sending $m \to \infty$, so think of m as large. The weak Mordell-Weil theorem says that the quotient group $E(K)/mE(K)$ is finite. Thus, some coset contains infinitely many P_i. Let's then pass to the subsequence contained in that coset, so that we have

$$P_i = [m]P_i' + R,$$

with $P_i', R \in E(K)$, and R independent of i. Then

$$\begin{aligned} m^2 h_f(P_i') &= h_f([m]P_i') + O(1) \\ &= h_f(P_i - R) + O(1) \\ &\leq 2h_f(P_i) + O(1), \end{aligned}$$

where this uses properties of height functions that are outside the scope of this talk. Note that $O(1)$ is independent of i, and that this relies on Proposition VIII.6.4 in Silverman, which requires that f be even.

We now proceed with the analogous computation for distance functions. If P_i is v-adically bounded away from Q, then $\log d_v(P_i, Q)$ is bounded, so $L = 0$. Otherwise, we pass to a subsequence with $P_i \to_v Q$, and correspondingly $[m]P_i' \to_v Q - R$. There are m^2 possible mth roots of $Q - R$, so P_i' must accumulate to at least one; we can pass to this subsequence again, to get a point $Q' \in E(\bar{K})$ with

$$P_i' \to_v Q' \text{ and } Q = [m]Q' + R.$$

The map $E \to E$ with $P \mapsto [m]P + R$ is everywhere unramified, so by Proposition 3.4,

$$\lim_{i\to\infty} \frac{\log d_v(P_i, Q)}{\log d_v(P_i', Q')} = 1.$$

Combining this and the height inequality, we get

$$L = \lim_{i\to\infty} \frac{\log d_v(P_i, Q)}{h_f(P_i)} \geq \lim_{i\to\infty} \frac{\log d_v(P_i', Q')}{\frac{1}{2}m^2 h_f(P_i') + O(1)}.$$

Applying Roth's Theorem in the distance setting (proposition 3.5) to $P_i' \subseteq E(K)$ which converges v-adically to $Q' \in E(\bar{K})$, we get

$$\liminf_{i\to\infty} \frac{\log d_v(P_i', Q')}{[K:\mathbb{Q}]h_f(P_i')} \geq -2.$$

Combining these last two yields

$$L \geq -\frac{4[K:\mathbb{Q}]}{m^2}.$$

Sending $m \to \infty$ gives $L \geq 0$, as desired. □

5. Many Corollaries, Some Proven

Here, we put a bunch of consequences, so that you can see how cool Siegel's Theorem is. We'll also put some extensions that are not consequences. But let's start with consequences.

Corollary 5.1. *Let E/K be an elliptic curve with Weierstrass coordinates x and y, and let $S \subseteq M_K$ be a finite set of places containing M_K^∞. Let R_S be the ring of S-integers of K. Then*

$$|\{P \in E(K) : x(P) \in R_S\}| < \infty.$$

Proof. We apply Siegel's Theorem with $f = x$, which is even by the explicit coordinates for $-P$ in the group law.

Let $P_1, P_2, \cdots \in E(K)$ be a sequence of distinct points with $x(P_i) \in R_S$ and $h_x(P_i) \to \infty$. Then

$$h_x(P_i) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in S} \log \max \left\{1, |x(P_i)|_v^{n_v}\right\},$$

where we ignore terms with $v \notin S$ since for those, $|x(P_i)|_v \leq 1$. Since S is finite, there exists $v \in S$ such that the vth term in this sum is the biggest infinitely often; we pass to this subsequence, which we relabel as the original P_i's. Thus for this $v \in S$, we have

$$h_x(P_i) \leq \frac{\#S}{[K:\mathbb{Q}]} \log \max\{1, |x(P_i)|_v^{n_v}\}.$$

There are only finitely many points at height 0 by a result of chapter VIII, so again we can pass to the infinite subsequence where $\max\{1, |x(P_i)|_v^{n_v}\} = |x(P_i)|_v^{n_v}$ to get our sequence P_i with

$$h_x(P_i) \leq \#S \frac{n_v}{[K:\mathbb{Q}]} \log |x(P_i)|_v.$$

In particular, $|x(P_i)|_v \to \infty$. The only pole of x is O, so $d_v(P_i, O) \to 0$. Moreover, O is a pole of $x \in K(E)$ of order 2, so let's define our distance function

$$d_v(P_i, O) = \min\left\{|x(P_i)|_v^{-1/2}, 1\right\}.$$

Then for sufficiently large i, we have

$$\frac{-\log d_v(P_i, O)}{h_x(P_i)} = \frac{-\log |x(P_i)|_v^{-1/2}}{h_x(P_i)} = \frac{\log |x(P_i)|_v}{2h_x(P_i)} \geq \frac{1}{2\#S}.$$

But this contradicts Siegel's Theorem, which says that this logarithmic expression should approach 0 as i becomes large. □

Example 5.2 (Diophantine Equations but way more hardcore this time)**.** I'm agnostic about whether or not to prove this example here, and it'll probably come down to how much time I have, but Siegel's theorem says something about solutions to Diophantine equations that is much stronger than just the fact that there are finitely many integral points. Consider the Diophantine equation

$$y^2 = x^3 + Ax + B,$$

with $A, B \in \mathbb{Z}$ and $4A^3 + 27B^2 \neq 0$. The above corollary says that this only has finitely many solutions $x, y \in \mathbb{Z}$. But what if we actually just apply Siegel's theorem with $Q = 0$, $f = x$, and v the archimedean absolute value on Q? Let's label the nonzero rational points $P_1, P_2, \cdots \in E(\mathbb{Q})$ in order of nondecreasing height, and write $x(P_i) = \frac{a_i}{b_i} \in \mathbb{Q}$ in lowest terms. What we end up getting after a medium-length computation is that

$$\lim_{i \to \infty} \frac{\log |a_i|}{\log |b_i|} = 1.$$

In other words, when looking at the x-coordinates of rational points on an elliptic curve, the numerators and denominators tend to have about the same number of digits.

Theorem 5.3 (Shafarevich's Theorem)**.** *Let $S \subseteq M_K$ be a finite set of places containing M_K^∞. Then up to isomorphism over K, there are only finitely many elliptic curves E/K having good reduction at all primes not in S.*

Corollary 5.4 (Corollary to Shafarevich). *For a fixed elliptic curve E/K there are only finitely many elliptic curves E'/K that are K-isogenous to E.*

Corollary 5.5 (Serre). *Let E/K be an elliptic curve with no complex multiplication. For almost all primes l, $E[l]$ has no nontrivial $G_{\bar{K}/K}$-invariant subgroups, i.e. the representation of $G_{\bar{K}/K}$ one $E[l]$ is irreducible.*

Now let's list some extensions. In general, the finiteness of S-integral points on elliptic curves is a special case of Siegel's general result that an affine curve C/K of genus at least one has finitely many S-integral points. For curves of genus two or more, this is superseded by Falting's theorem, which says that the set of rational points $C(K)$ is finite.

But Siegel also provided an alternative proof for a broader class of curves that includes elliptic curves. Here are some of those results.

Theorem 5.6. *Let $S \subseteq M_K$ be a finite set of places, and let $a, b \in K^*$. The equation $ax + by = 1$ has finitely many solutions in $x, y \in R_S^*$.*

Theorem 5.7 (Siegel). *Let $f(x) \in K[x]$ be a polynomial of degree at least 3 with distinct roots in $\bar{K}$. The equation $y^2 = f(x)$ has only finitely many solutions $x, y \in R_S$.*

Corollary 5.8. *Let C/K be a curve of genus one with $f \in K(C)$ a nonconstant function. There are finitely many points $P \in C(K)$ with $f(P) \in R_S$.*

References

[1] Hashimoto, Sachi, 2014. The ABC Conjecture and its Consequences on Curves. http://math.bu.edu/people/svh/AGFinalPaper.pdf.

[2] Silverman, Joseph, 1986. The Arithmetic of Elliptic Curves. *Springer-Verlag.*