MA 254 notes: Diophantine Geometry
(Distilled from [Hindry-Silverman])

Dan Abramovich

Brown University

March 20, 2016

The S-unit equation

Theorem (Siegel-Mahler)

Let K bye a number field, $S \subset M_K$ a finite set of places, $S \supset M_K^\infty$. The equation

$$U + V = 1$$

has finitely many solutions with $U, V \in \mathcal{O}_{K,S}^\times$.

Exercise

The same holds for $aU + bV = c$ with $a, b, c \in K^\times$.

We will pass to an infinite subset of solutions by mapping the solutions to the finite set $\left(\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^m\right) \times S \times \mu_m$. We will choose the integer $m > 2|S|$.

Pigeon holes: units modulo mth powers

- For ease of notation we replace V by $-V^{-1}$ and consider the equation $U - V^{-1} = 1, U, V \in \mathcal{O}_{K,S}^\times$.
- We argue by contradiction and assume there are infinitely many $(U, V) \in \mathcal{O}_{K,S}^\times$ solving this.
- Note that $\mathcal{O}_{K,S}^\times \simeq \mathbb{Z}^{|S|-1} \times \mu(K)$ is finitely generated, so the set $\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^m$ is finite. Let $\Omega_1 \subset \mathcal{O}_{K,S}^\times$ be a set of representatives.
- It follows that there is $(a, b) \in \Omega^2$ such that for infinitely many solutions U, V we have $aU, bV \in (\mathcal{O}_{K,S}^\times)^m$.
- We therefore have infinitely many $X, Y \in \mathcal{O}_{K,S}^\times$ with $\frac{X^m}{a} - \frac{b}{Y^M} = 1$, and writing $Z = XY$ we have

$$Z^m - ab = aY^m.$$

Pigeon holes: S

- For each $v \in S$ consider the values $\|Y\|_v$.
- Given a solution X, Y (or Y, Z) there is a $w \in S$ where $\|Y\|_v$ is minimal.
- Since $\|Y\|_{v'} = 1$ for $v' \notin S$ and since $\prod_{v \in M_k} \|Y\|_v = 1$, this is in fact the minimum over all M_K, and $\|Y\|_w < 1$.
- Since there are infinitely many solutions and S is finite, there is w so that infinitely many solutions have $\{\|Y\|_v\}$ take its minimum at $\|Y\|_w$.
- We consider that infinite subset of solutions of $Z^m - ab = aY^m$.

The trick, and the final pigeon holes in μ_m

- Write $\alpha = (ab)^{1/m}$. The equation becomes

$$\prod_{i=0}^{m-1} (Z - \zeta_m^i \alpha) = aY^m. \tag{1}$$

- There is $0 \leq i \leq m-1$ with an infinite subset of solutions so that $\|Z - \zeta_m^j \alpha\|_w$ obtains its minimum at i. Renaming α to be this $\zeta_m^i \alpha$, we may assume $i = 0$.
- We will show that the Z in this sequence approximate α too well at w.
- Note that Z does not approximate $\zeta_m^j \alpha, j \neq 0$ at w: we have

$$\begin{aligned} |Z - \zeta^j \alpha|_w &\geq (1/2)|\alpha - \zeta^j \alpha|_w & (2)\\ &\geq (1/2) \min_j |\alpha - \zeta^j \alpha|_w = C > 0. & (3) \end{aligned}$$

Estimates

- Equation (1) and the bound (2) imply that
$$|Z-\alpha|_w \le (C^{1-m}|a|_w)|Y^m|_w := C'|Y^m|_w.$$
- Raising to the appropriate power we have
$$\|Z-\alpha\|_w \le C''\|Y^m\|_w. \tag{4}$$
- Note
$\|Y\|_w = \min\{\|Y\|_v : v \in S\} \le \left(\prod_{v\in S} \min(\|Y\|_v, 1)\right)^{1/|S|} = \left(\prod_{M_K} \min(\|Y\|_v, 1)\right)^{1/|S|} = H_K(Y)^{-1/|S|}.$

Estimates, continued

- Recall that $H_K(xy) \leq H_K(x)H_K(y)$. We also have as exercise $H_K(x+y) \leq 2^{[K:\mathbb{Q}]}H_K(x)H_K(y)$.
- Now $H_K(Z)^m = H_K(Z^m) = H_K(aY^m - ab) \leq 2^{[K:\mathbb{Q}]}H_K(Y^m)H_K(a)H_K(ab) = DH_K(Y)^m$,
- in other words $H_K(Z) \leq D'H_K(Y)$.
- Writing $C''' = (C''/D^{1/|S|})^m$ we get

$$\begin{aligned} \|Z - \alpha\|_w \leq C''\|Y^m\|_w &\leq C''H_K(Y)^{-m/|S|} \\ &\leq C'''H_K(Z)^{-m/|S|} \end{aligned}$$

- If we take from the outset, as promised, $m \geq 2|S| + 1$ and write $\epsilon = 1/|S|$, we get infinitely many $Z \in K$ with

$$\|Z - \alpha\|_w \leq C'''/H_K(Z)^{2+\epsilon},$$

contradicting Roth's theorem.