$\mathfrak{p}$-adic Numbers and Skolem's Method

Daniel Grunkin

University of Copenhagen

June 21, 2024

What we will cover

Diophantine equations

What is a Diophantine equation?

Diophantine equations

Question: Given a Diophantine equation, can we determine if it has infinitely many solutions?

Hilbert's 10th problem

There is no algorithm that can determine if an arbitrary Diophantine equation has a solution.

An equation where we can answer the question

Consider the equation

$$x^2 - 2y^2 = 7.$$

A solution is $x = 3$ and $y = 1$ and if (x, y) is a solution then so is $(3x + 4y, 2x + 3y)$. Thus, there are infinitely many solutions to this equation.

Another approach

Let $K = \mathbb{Q}(\sqrt{2})$. Then

$$N_{K/\mathbb{Q}}(x + y\sqrt{2}) = x^2 - 2y^2$$

Let $\mathfrak{D}$ be the coefficient ring for $\langle 1, \sqrt{2} \rangle$. By Dirichlet's Unit theorem

$$\mathfrak{D}^* = W \times V$$

with W finite and V free abelian with rank $r + s - 1 = 2 + 0 - 1 = 1$.
Consider again

$$x^2 - 2y^2 = 7$$

Consider Pell's equation $x^2 - ny^2 = 1$, n not a square.

A more general case

Let K be a number field, $\mu_1, ..., \mu_n$ a basis and assume

$$F(x_1, ..., x_n) = N_{K/\mathbb{Q}}(x_1\mu_1 + \cdots + x_n\mu_n)$$

Does $F(x_1, ..., x_n) = c$, $c \in \mathbb{Q}$, have infinitely many solutions?

Let $M = \langle \mu_1, ..., \mu_n \rangle$. Then there is a finite set Γ of elements of norm c and independent units of norm 1, $\epsilon_1, ..., \epsilon_t \in \mathfrak{D}^*$, so that for all $\alpha \in M$ we have

$$N_{K/\mathbb{Q}}(\alpha) = c$$

if and only if

$$\alpha = \gamma \epsilon_1^{u_1} ... \epsilon_t^{u_t}$$

Here $t = r + s - 1$. So to answer the question...

Thue's Theorem

Theorem (Thue)

Suppose $f(x, y)$ is an irreducible form of degree $n \geq 3$. Then there are only finitely many integer solutions to the equation $f(x, y) = c$, for any non-zero $c \in \mathbb{Q}$.

With the additional requirement that $f(x, 1)$ has an imaginary root, Thoralf Skolem proved this theorem.

Some general considerations

Suppose K is a number field with basis $\mu_1, ..., \mu_n$ and suppose F is an irreducible form so that $F(x_1, ..., x_m) = N_{K/\mathbb{Q}}(x_1\mu_1 + \cdots + x_m\mu_m)$ with $m < n$. Consider the equation

$$F(x_1, ..., x_m) = c$$

Does this equation have finitely many solutions?

Let

$$M = \langle \mu_1, \ldots, \mu_m \rangle \text{ and } M' = \langle \mu_1, \ldots, \mu_m, \mu_{m+1}, \ldots, \mu_n \rangle$$

Finding the solutions to

$$F(x_1, ..., x_m) = c$$

is the same as finding $\alpha := x_1\mu_1 + ... + x_n\mu_n \in M'$ so that $N_{K/\mathbb{Q}}(\alpha) = c$ under the requirement

$$x_{m+1} = ... = x_n = 0$$

Now,

$$x_{m+1} = ... = x_n = 0$$

is the same as

$$\mathrm{Tr}_{K/\mathbb{Q}}(\mu^*_{m+1}\alpha) = ... = \mathrm{Tr}_{K/\mathbb{Q}}(\mu^*_n\alpha) = 0$$

which is again the same as the equations

$$\sum_{j=1}^{n} \sigma_j(\mu_i^*\alpha) = 0, \text{ for } i \in \{m+1, ..., n\}$$

Since $\alpha \in M'$ and $N_{K/\mathbb{Q}}(\alpha) = c$ we can write

$$\alpha = \gamma \epsilon_1^{u_1} \ldots \epsilon_t^{u_t}$$

for $u_i \in \mathbb{Z}$ and $\gamma \in \Gamma$. So

$$\sum_{j=1}^{n} \sigma_j(\gamma \mu_i^*) \sigma_j(\epsilon_1)^{u_1} \ldots \sigma_j(\epsilon_t)^{u_t} = \sum_{j=1}^{n} \sigma_j(\mu_i^* \alpha) = 0, \text{ for } i \in \{m+1, \ldots, n\}.$$

Suppose $K = \mathbb{Q}(\beta)$ and set $N = \mathbb{Q}(\sigma_1(\beta), \ldots, \sigma_n(\beta))$. Pick a prime $\mathfrak{p}$ of O_N. We get a valuation $v_{\mathfrak{p}}$ on N and it extends to the completion $N_{\mathfrak{p}}$. Let $O_{\mathfrak{p}}$, the valuation ring in $N_{\mathfrak{p}}$.

Consider again

$$\sum_{j=1}^{n} \sigma_j(\gamma\mu_i^*)\sigma_j(\epsilon_1)^{u_1}...\sigma_j(\epsilon_t)^{u_t} = 0$$

The $\epsilon_i \in \mathfrak{D}^*$ can be chosen so that it makes sense to allow $u_i \in O_{\mathfrak{p}}$. Setting $A_{ij} = \sigma_j(\gamma\mu_i^*)$ and $L_j(u_1, ..., u_t) = \sum_{i=1}^{t} u_i \log(\sigma_j(\epsilon_i))$ we now define

$$G_i(u_1, ..., u_t) := \sum_{j=1}^{n} A_{ij} \exp L_j(u_1, ..., u_t)$$

Suppose $F(x_1, ..., x_m) = c$ has infinitely many solutions. Then there is $\gamma \in \Gamma$ so that $S_\gamma = \{\gamma\epsilon_1^{u_1}...\epsilon_t^{u_t} \mid u_i \in \mathbb{Z}\} \subseteq M$ is an infinite set of elements with norm c. We have an injective homomorphism $\iota : S_\gamma \hookrightarrow O_\mathfrak{p}^t$. Let α_s be a sequence of unique elements of S_γ. Then $U_s = \iota(\alpha_s)$ is a sequence of unique elements of $O_\mathfrak{p}^t$. Hence there is a convergent subsequence U_s^* of U_s converging to $u^* = (u_1^*, ..., u_t^*) \in O_\mathfrak{p} \implies$ infinitely many points in any neighborhood of u^*. Note also that we now have a subsequence α_s^* of α_s so that $U_s^* = \iota(\alpha_s^*)$.

Shifting to the origin

Let $(u_1, \ldots, u_t) \in O_{\mathfrak{p}}^t$ and write $u_k = u_k^* + v_k$ and set $A_{ij}^* = A_{ij} \exp L_j(u_1^*, \ldots, u_t^*)$. We get for $i \in \{m+1, \ldots, n\}$

$$G_i(u_1, \ldots, u_t) = \sum_{j=1}^{n} A_{ij}^* \exp L_j(v_1, \ldots, v_t) =: H_i(v_1, \ldots, v_t)$$

The H_i define a local manifold, V, and it contains infinitely many points in any ϵ-neighborhood of the origin. Hence V contains an analytic curve.

Let us continue...

Let W be the local manifold given by

$$\prod_{i \leq k < l \leq n} (L_k(v_1, ...v_t) - L_l(v_1, ..., v_t)) = 0$$

Let W be the local manifold given by

$$\prod_{i \leq k < l \leq n} (L_k(v_1, \ldots v_t) - L_l(v_1, \ldots, v_t)) = 0$$

Assume $\omega_1(X), \ldots, \omega_t(X)$ is a curve on V.

Let W be the local manifold given by

$$\prod_{i \le k < l \le n} (L_k(v_1, \ldots v_t) - L_l(v_1, \ldots, v_t)) = 0$$

Assume $\omega_1(X), \ldots, \omega_t(X)$ is a curve on V. This means that we have

$$\sum_{j=1}^{n} A^*_{ij} \exp L_j(\omega_1(X), \ldots, \omega_t(X)) = 0$$

for $i = m + 1, \ldots, n$.

Let W be the local manifold given by

$$\prod_{i \leq k < l \leq n} (L_k(v_1, \ldots v_t) - L_l(v_1, \ldots, v_t)) = 0$$

Assume $\omega_1(X), \ldots, \omega_t(X)$ is a curve on V. This means that we have

$$\sum_{j=1}^{n} A_{ij}^{*} \exp L_j(\omega_1(X), \ldots, \omega_t(X)) = 0$$

for $i = m+1, \ldots, n$. **Suppose we have $k \neq l$ so that**

$$L_k(\omega_1(X), \ldots, \omega_t(X)) = L_l(\omega_1(X), \ldots, \omega_t(X))$$

In other words, under our assumption, if a curve is on V then it is also on W so $V \subseteq W$.

Write

$$\iota(\alpha_s^*) = (u_{1s}, ..., u_{ts})$$
$$u_{is} = u_i^* + v_{is}$$

Set $V_s = (v_{1s}, ..., v_{ts})$. Then $V_s \in V$ converges to the origin so there is $N \in \mathbb{N}$ so that $V_s \in W$ for all $s \geq N$. Thus there are $k \neq l$ so that $L_k(V_s) - L_l(V_s) = 0$ for all $s \geq N$. Consider

$$\{\alpha_s^* \mid L_k(V_s) - L_l(V_s) = 0 \text{ for } s \geq N\}$$

If this is a finite set then $F(x_1, ..., x_m) = c$ has finitely many solutions.

A case where we can overcome the two obstructions

If $m = 2$ and one of the σ_j is a complex embedding, then we can overcome these obstructions. Let us see why.

In this case, consider again

$$\{\alpha_s^* \mid L_k(V_s) - L_l(V_s) = 0 \text{ for } s \geq N\}$$

Why is this set finite?

We also need to show that there exists $k \neq l$ so that

$$L_k(\omega_1(X), ..., \omega_t(X)) = L_l(\omega_1(X), ..., \omega_t(X))$$

A consequence of what we have just shown

Let $\omega_1(X), \ldots, \omega_t(X)$ be a curve on V. Define $P_j(X) = L_j(\omega_1(X), \ldots, \omega_t(X))$ for $j \in \{1, \ldots, n\}$. There exists a matrix B_{ij} with linearly independent rows so that

$$\sum_{j=1}^{n} A_{ij}^{*} \exp P_j = 0, \text{ for all } i \in \{m+1, \ldots, n\}$$

$$\sum_{j=1}^{n} B_{ij} P_j = 0, \text{ for all } i \in \{1, \ldots, n-t\},$$

The matrix (A_{ij}^{*}) has linearly independent rows.

A useful lemma

Let L be a field of characteristic 0 and let $n, n_1, n_2 \in \mathbb{N}$ so that $n_1 = n - 2$ and $n_2 \geq 2$ and suppose we have formal power series, $P_1, ..., P_n \in L[[X]]$ with zero constant term so that

$$\sum_{j=1}^{n} a_{ij} \exp P_j = 0, \text{ for all } i \in \{1, ..., n_1\}$$

$$\sum_{j=1}^{n} b_{ij} P_j = 0, \text{ for all } i \in \{1, ..., n_2\},$$

where both matrices (a_{ij}) and (b_{ij}) have linearly independent rows. Then there are two indices $k \neq l$ so that $P_k = P_l$.

Let us compare the last two slides

We have $t = r + s - 1$ and $n = 2s + r$. Set $n_1 = n - m$ and $n_2 = n - t$. To apply the lemma we need $m = 2$. Also, $n_1 \in \mathbb{N}$ if and only if $n_1 = n - 2 \geq 1$ if and only if $n \geq 3$. We also have $n_2 = 2s + r - (r + s - 1) = s + 1$. So $n_2 \geq 2$ if and only if $s \geq 1$.

Conclusion: The lemma can be applied with $n_1 = n - 2$ and $n_2 = n - t$ if and only if there is at least one pair of complex conjugate embeddings and $n \geq 3$.

Thue's Theorem

Theorem (Thue)

Suppose $f(x, y)$ is an irreducible form of degree $n \geq 3$ and $f(x, 1)$ has an imaginary root. Then there are only finitely many integer solutions to the equation $f(x, y) = c$, for any non-zero $c \in \mathbb{Q}$.

Proof of Thue's theorem

Let θ be a root of $f(x,1)$. First show that $f(x,y) = N_{K/\mathbb{Q}}(x + y\theta)$ with $K = \mathbb{Q}(\theta)$. We the special case from before.

The general case again

Suppose K is a number field with basis $\mu_1, ..., \mu_n$ and suppose F is an irreducible form so that $F(x_1, ..., x_m) = N_{K/\mathbb{Q}}(x_1\mu_1 + \cdots + x_m\mu_m)$ with $m < n$. Consider the equation

$$F(x_1, ..., x_m) = c$$

Does this equation have finitely many solutions?

Consider the equation

$$N_{\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}}(x + y\sqrt{2} + z\sqrt{3}) = 1$$

Setting $z = 0$ we have

$$\begin{aligned} N_{\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}}(x + y\sqrt{2}) &= N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(N_{\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}(\sqrt{2})}(x + y\sqrt{2})) \\ &= N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}((x + y\sqrt{2})^2) \\ &= N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(x + y\sqrt{2})^2 = 1 \end{aligned}$$

Definition

Let K be a number field and M a module with generators $\mu_1, \ldots, \mu_m$ and consider the vector space $L = \mathrm{span}_{\mathbb{Q}}\{\mu_1, \ldots, \mu_m\}$. If L contains a subspace L' so that $\gamma K' = L'$ for some subfield K' of K and $\gamma \in K$ and K' is neither $\mathbb{Q}$ or a quadratic imaginary field then we say that M is degenerate. Otherwise the module is called non degenerate.

Proposition

Suppose $M \subseteq K$ is degenerate. Then there is $c \in \mathbb{Q}$ so that

$$N_{K/\mathbb{Q}}(\beta) = c$$

for infinitely many $\beta \in M$.

Proof.

Suppose $M \subseteq K$ is degenerate and let K' be a subfield of K and L' be a subspace of L so that $\gamma K' = L'$, with K' neither $\mathbb{Q}$ or a quadratic imaginary field. Define $M' = M \cap L'$. We have $K' = \gamma^{-1} L'$ so $\gamma^{-1} M'$ is a full module inside K'. Suppose

$$N_{K'/\mathbb{Q}}(\alpha) = c$$

for $\alpha \in \gamma^{-1} M'$. We have $\alpha\gamma \in M' \subseteq M$. Note that $\alpha \in \gamma^{-1} L' = K'$ so $N_{K/K'}(\alpha) = \alpha^m$ ($m = [K : K']$). Thus

$$N_{K/\mathbb{Q}}(\alpha) = N_{K'/\mathbb{Q}}(N_{K/K'}(\alpha)) = N_{K'/\mathbb{Q}}(\alpha^m) = c^m$$

So

$$N_{K/\mathbb{Q}}(\gamma\alpha) = N_{K/\mathbb{Q}}(\gamma) N_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\gamma) c^m$$

□

Conjecture: Let $F(x_1, ..., x_m) = N_{K/\mathbb{Q}}(x_1\mu_1 + ... + x_m\mu_m)$. Perhaps $F(x_1, ..., x_m) = c$ has finitely many solutions if $\langle \mu_1, ..., \mu_m \rangle$ is non-degenerate and F irreducible?

Conjecture: Let $F(x_1, \dots, x_m) = N_{K/\mathbb{Q}}(x_1\mu_1 + \dots + x_m\mu_m)$. Perhaps $F(x_1, \dots, x_m) = c$ has finitely many solutions if $\langle \mu_1, \dots, \mu_m \rangle$ is non-degenerate and F irreducible?

- This is true when K is a quadratic imaginary field or $\mathbb{Q}$.
- We already know this is true when $m = 2$ and $n \geq 3$.

Conjecture: Let $F(x_1, ..., x_m) = N_{K/\mathbb{Q}}(x_1\mu_1 + ... + x_m\mu_m)$. Perhaps $F(x_1, ..., x_m) = c$ has finitely many solutions if $\langle \mu_1, ..., \mu_m \rangle$ is non-degenerate and F irreducible?

- This is true when K is a quadratic imaginary field or $\mathbb{Q}$.
- We already know this is true when $m = 2$ and $n \geq 3$.
- Using different techniques this is valid for $m = 3$.

Conjecture: Let $F(x_1, ..., x_m) = N_{K/\mathbb{Q}}(x_1\mu_1 + ... + x_m\mu_m)$. Perhaps $F(x_1, ..., x_m) = c$ has finitely many solutions if $\langle \mu_1, ..., \mu_m \rangle$ is non-degenerate and F irreducible?

- This is true when K is a quadratic imaginary field or $\mathbb{Q}$.
- We already know this is true when $m = 2$ and $n \geq 3$.
- Using different techniques this is valid for $m = 3$.

How to proceed?: A place to start could be to try to prove/disprove this for when n, the degree of K, is a prime. An alternative is to strengthen the lemma we used in the proof of Thue's theorem.

Improvements of lemma

Recall that we want $H_i(v_1, ..., v_t) = 0$, $i \in \{1 + m, ..., n\}$. So we have $n - m$ equations in t variables. What happens when $n - m \geq t$?

Note that $n - m \geq t$ if and only if

$$(2s + r) - m \geq r + s - 1$$

if and only if

$$s \geq m - 1$$

If we set $n_1 = n - m$ and $n_2 = n - t$ then $n_1 + n_2 = 2n - m - t$. Thus $n_1 + n_2 \geq n$ if and only if $n - m \geq t$.

Upgrade of lemma

Let L be a field of characteristic 0 and let $n, n_1, n_2 \in \mathbb{N}$ so that $\cancel{n_1 = n - 2}$ ~~and~~ $\cancel{n_2 \geq 2}$ $n_1 + n_2 \geq n$ and suppose we have formal power series, $P_1, \ldots, P_n \in L[[X]]$ with zero constant term so that

$$\sum_{j=1}^{n} a_{ij} \exp P_j = 0, \text{ for all } i \in \{1, \ldots, n_1\}$$

$$\sum_{j=1}^{n} b_{ij} P_j = 0, \text{ for all } i \in \{1, \ldots, n_2\},$$

with the a_{ij} and b_{ij} in L and where both matrices (a_{ij}) and (b_{ij}) have L-linearly independent rows. Then there are two indices $k \neq l$ so that $P_k = P_l$.

Thus, if the upgraded lemma was true and if $s \geq m - 1$, we would be able to get past the first obstruction. It has been shown that the lemma holds in the special case where $n = 5, n_1 = 2, n_2 = 3$.

Improvements by Alan Baker

Theorem

Assume K is a number field of degree d, let $\alpha_1, \ldots, \alpha_n$ be distinct elements in O_K with $n \geq 3$ and let $\mu \in O_K$, $\mu \neq 0$. Then

$$(x - \alpha_1 y) \ldots (x - \alpha_n y) = \mu$$

has finitely many solutions with $x, y \in O_K$ and these can be determined.

- Equation need not have coefficients in $\mathbb{Q}$.
- x, y can take values in O_K, not just $\mathbb{Z}$.
- The solutions can be determined.