Diophantine Problems

A Diophantine problem is the question about the rational (integral) solutions for a system of equations given by :

$$f_i(x_1, \cdots, x_n) = 0, \; i = 1, \cdots, m$$

over $\mathbb{Q}$ or number fields ($\mathbb{Z}$ or ring of integers) or for a family of such systems.

Hilbert's 10th problem

Does there exist an algorithm to decide the solubility of each Diophantine problem?

- **Answer over $\mathbb{Z}$:** No

  In other words, there is an equation $p(c; x_1, \cdots, x_m)$ over $\mathbb{Z}$ such that there is no algorithm to decide the solubility for given c.

- **Answer over $\mathbb{Q}$:** Not found yet

  Sir Peter says he is in the minority who believe the answer over $\mathbb{Q}$ is "yes"

General questions on Diophantine problems

1. For the given family, is there an algorithm deciding the solubility?
2. If the system is soluble, is there an algorithm to find a solution?
3. Can you describe all solutions?

Hasse Principle

For any Diophantine equation, solubility over $\mathbb{Q}$ implies solubility over $\mathbb{Q}_v$ for each place v of $\mathbb{Q}$.

The Hasse principle for a family of Diophantine problems $\mathfrak{F}$ means

- V in $\mathfrak{F}$ is soluble over $\mathbb{Q} \iff V$ is soluble over each $\mathbb{Q}_v$.

What makes the Hasse principle valuable is that, for any given single Diophantine problem, there is an algorithm deciding local solublility. The Hasse principle holds for the family of quadrics of any dimension.

Hilbert Symbol

- Let $c_1, c_2 \in \mathbb{Q}^*$. Hilbert symbol $(c_1, c_2)_v$ is defined as

$$
\begin{aligned}
(c_1, c_2)_v &= 1 \quad \text{if } c_1 x_1^2 + c_2 x_x^2 = 1 \text{ is soluble in } \mathbb{Q}_v \\
&= -1 \quad \text{otherwise}
\end{aligned}
$$

- Hilbert product formula
  $\prod_v (c_1, c_2)_v = 1$
- $a_0 x_0^2 + a_1 x_1^2 + a_2 x_2^2 = 0$ is soluble iff $(-a_0 a_1, -a_0 a_2)_v = 1$ for every v, since the quadric satisfies the Hasse principle.

Classification of Diophantine problems w.r.t geometric properties

- Dimension 1 : curve

genus	$= 0$	conic
	$= 1$	elliptic curve; detail structure is conjectured by Birch and Swinnerton-Dyre
	> 1	hyperelliptic curve; Faltings theorem

- Dimension 2 : surface

  The classification is not yet completed.

  There have been studies on some rational surfaces such as

  - pencils of conics
  - Del Pezzo surfaces

A pencil of conics is a family of conics fibered by $\mathbb{P}^1$.

Pencil of conics is given by the equation :

$$V : a_0(U,V)X_0^2 + a_1(U,V)x_1^2 + a_2(U,V)x_2^2 = 0,\ a_i \in \mathbb{Z}[U,V].$$

We may assume the a_i's are square free, coprime to each other and homogenous with degree of the same parity.

$\mathcal{B}$ = The finite set of places which consists of 2,∞ and primes mod which the reduction of $a_0a_1a_2$ is not separable.

Let $\mathcal{N}$ be the subset in $\mathbb{Z}\times\mathbb{Z}$ consisting of $\alpha\times\beta\in\mathcal{N}$ at which V is soluble over $\mathbb{Q}_v$ for each $v\in\mathcal{B}$. Then $\mathcal{N}$ is open in the $\mathcal{B}$-adic topology.

For a given $\alpha \times \beta \in \mathcal{N}$, $V(\alpha, \beta)$ is soluble over $\mathbb{Q}_p$ where $p \notin \mathcal{B}$ iff

a. p does not divide $(a_0 a_1 a_2)$ or
b. if p divides $c(\alpha, \beta)$ where c is an irreducible factor of a_2,
then $(-a_0(\alpha, \beta) a_1(\alpha, \beta), c(\alpha, \beta))_p = 1$.

So a necessary condition for the solubility of V at $\alpha \times \beta$ is

- $L(\mathcal{B}; -a_0 a_1, c; \alpha, \beta) = \prod_{p \notin \mathcal{B},\ p | c(\alpha,\beta)} (-a_0 a_1, c)_p = 1$

Lemma $L(\mathcal{B}; -a_0 a_1, c; \alpha, \beta)$ is continuous in the topology induced by $\mathcal{B}$.