3

The local-global principle for conics

We have seen that the theory of curves of genus 0 over $\mathbf{Q}$ turns on deciding whether a given conic has a rational point.

We use homogeneous co-ordinates. A conic C defined over $\mathbf{Q}$ is given by an equation

$$F(\mathbf{X}) = \sum f_{ij} X_i X_j = 0$$

where $\mathbf{X} = (X_1, X_2, X_3)$,

$$f_{ij} = f_{ji} \in \mathbf{Q}$$

and the quadratic form F (recall a *form* is a homogeneous polynomial) is nonsingular, i.e.

$$\det(f_{ij}) \neq 0.$$

In our initial discussion we noted that, apart from reality considerations, we could disprove the existence of rational points by congruence considerations. These we now replace by reference to p-adic numbers.

A criterion for the existence of a rational point on a conic was given by Legendre. It was left to Hasse to give it the following succinct formulation.

Theorem 1. *A necessary and sufficient condition for the existence of a rational point on a conic C defined over $\mathbf{Q}$ is that there is a point defined over the real field $\mathbf{R}$ and over $\mathbf{Q}_p$ for every prime p.*

Necessity is trivial. We shall prove sufficiency, but it will require some time and preparation. First we introduce some conventional terminology.

 https://doi.org/10.1017/CBO9781139172530.004

The real field $\mathbf{R}$ is somewhat analogous to the $\mathbf{Q}_p$ and is conventionally denoted by $\mathbf{Q}_\infty$. When we write $\mathbf{Q}_p$ we will not include $p = \infty$ unless we explicitly say so. The fields $\mathbf{Q}_p$ (including $p = \infty$) are called the localizations of $\mathbf{Q}$. In contrast, $\mathbf{Q}$ is called the global field. We say that something is true "everywhere locally" if it is true for all $\mathbf{Q}_p$ (including ∞). In this lingo the theorem becomes "A necessary and sufficient condition for the existence of a global point on a conic is that there should be a point everywhere locally".

The local-global theorem for conics implies a local-global theorem for curves of genus 0 but some care must be taken in the formulation ["point" must be interpreted as "place"]. We do not pursue this further.

In the rest of this section we transform the theorem into a shape better suited for attack[1].

A transformation

$$T: \ X_i = \sum_i t_{ij} Y_j$$

with

$$t_{ij} \in \mathbf{Q}, \qquad \det(t_{ij}) \neq 0$$

takes the quadratic form $F(\mathbf{X})$ into a quadratic form $G(\mathbf{Y})$, say. Then T takes points defined over $\mathbf{Q}$ on $F(\mathbf{X}) = 0$ into points defined over $\mathbf{Q}$ on $G(\mathbf{Y}) = 0$ and, similarly, the inverse T^{-1} takes points on $G(\mathbf{Y}) = 0$ to points on $F(\mathbf{X}) = 0$. Likewise for points defined over $\mathbf{Q}_p$ for each p (including ∞). Hence the theorem holds for $F(\mathbf{X}) = 0$ if and only if it holds for $G(\mathbf{Y}) = 0$.

By suitable choice of transformation T we thus need consider only "diagonal" forms

$$F(\mathbf{X}) = f_1 X_1^2 + f_2 X_2^2 + f_3 X_3^2.$$

By substitutions $X_j \to t_j X_j$ ($t_j \in \mathbf{Q}$) we may suppose without loss of generality that the

$$f_j \in \mathbf{Z}$$

are square free.

If f_1, f_2, f_3 have a prime factor p in common, we replace $F(\mathbf{X})$ by $p^{-1}F(\mathbf{X})$. If two of the f_j, say f_1, f_2 have a prime p in common but $p \nmid f_3$, we replace X_3 by pX_3 and then divide F by p. Both of these

[1] The details of the proof of Theorem 1 will not be required for the treatment of elliptic curves. The reader who is interested only in the latter should omit the rest of this § and also omit §§4,5.

transformations reduce the absolute value of the integer $f_1 f_2 f_3$. After a finite number of steps we are reduced to the case when $f_1 f_2 f_3$ is square free. We have thus proved the

Metalemma 1. *To prove the Theorem, it is enough to prove it for conics*

$$F(\mathbf{X}) = f_1 X_1^2 + f_2 X_2^2 + f_3 X_3^2 = 0,$$

where $f_j \in \mathbf{Z}$ and $f_1 f_2 f_3$ is square free.

The next stage is to draw conclusions from the hypothesis that a conic as described in the Metalemma has points everwhere locally. There is a point defined over $\mathbf{Q}_p$ when there is a vector $\mathbf{a} = (a_1, a_2, a_3) \neq (0,0,0)$ with $a_j \in \mathbf{Q}_p$ such that $F(\mathbf{a}) = 0$. By multiplying the a_j by an element of $\mathbf{Q}_p$ we may suppose without loss of generality that

$$\max |a_j|_p = 1. \qquad (*)$$

For our later purposes we have to consider several cases.

First case. $p \neq 2$, $p \mid f_1 f_2 f_3$. Without loss of generality $p \mid f_1$, so $p \nmid f_2$, $p \nmid f_3$. Then $|f_1 a_1^2|_p < 1$. Suppose, if possible that $|a_2|_p < 1$. Then

$$|f_3 a_3^2|_p = |f_1 a_1^2 + f_2 a_2^2|_p < 1$$

and $|a_3|_p < 1$. Now

$$|f_1 a_1^2|_p = |f_2 a_2^2 + f_3 a_3^2|_p \leq p^{-2}$$

and so $|a_1|_p < 1$ since f_1 is square free. This contradicts the normalization (*), and so $|a_2|_p = |a_3|_p = 1$. But now

$$|f_2 a_2^2 + f_3 a_3^2|_p < 1.$$

On dividing by the unit a_2, we deduce that there is some $r_p \in \mathbf{Z}$ such that

$$f_2 + r_p^2 f_3 \equiv 0\ (p).$$

Second case. $p = 2$, $2 \nmid f_1 f_2 f_3$. It is easy to see that precisely two of the a_j are units, say a_2 and a_3. Now $a^2 \equiv 1$ or 0 (4) for $a \in \mathbf{Z}$; and so

$$f_2 + f_3 \equiv 0\ (4).$$

Third case. $p = 2$, $2 \mid f_1 f_2 f_3$, say $2 \mid f_1$. Now $|a_2|_2 = |a_3|_3 = 1$. Now $a^2 \equiv 1$ (8) for $a \in \mathbf{Z}$, $2 \nmid a$; and so

$$f_2 + f_3 \equiv 0\ (8)$$

or

$$f_1 + f_2 + f_3 \equiv 0\ (8)$$

according as $|a_1|_2 < 1$ or $|a_1|_2 = 1$.

In the next two sections, we show that the conditions just derived are sufficient to ensure the existence of a global point on $F(\mathbf{X}) = 0$.

§3. Exercises

1. (i) Let $p > 2$ be prime and let b, $c \in \mathbb{Z}$, $p \not| \, b$. Show that $bx^2 + c$ takes precisely $\frac{1}{2}(p+1)$ distinct values p for $x \in \mathbb{Z}$. (ii) Suppose that, further, $a \in \mathbb{Z}$, $p \not| \, a$. Show that there are x, $y \in \mathbb{Z}$ such that $bx^2 + c \equiv ay^2 \ (p)$.

2. Let a, b, $c \in \mathbb{Z}_p$, $|a|_p = |b|_p = |c|_p = 1$ where p is prime, $p > 2$. Show that there are x, $y \in \mathbb{Z}_p$ such that $bx^2 + c = ay^2$.

3. Let $p > 2$ be prime, $a_{ij} \in \mathbb{Z}$ $(1 \le i, j \le 3)$, $a_{ji} = a_{ij}$ and let $d = \det(a_{ij})$. Suppose that $p \not| \, d$. Show that there are x_1, x_2, $x_3 \in \mathbb{Z}$, not all divisible by p, such that $\sum_{i,j} a_{ij} x_i x_j \equiv 0 \ (p)$.

4. Let a, b, $c \in \mathbb{Z}$, $2 \not| \, abc$. Show that a necessary and sufficient condition that the only solution in $\mathbb{Q}_2$ of $ax^2 + by^2 + cz^2 = 0$ is the trivial one is that $a \equiv b \equiv c \ (4)$.

5. For each of the following sets of a, b, c find the set of primes p (including ∞) for which the only solution of $ax^2 + by^2 + cz^2 = 0$ in $\mathbb{Q}_p$ is the trivial one:

(i) $(a, b, c) = (1, 1, -2)$
(ii) $(a, b, c) = (1, 1, -3)$
(iii) $(a, b, c) = (1, 1, 1)$
(iv) $(a, b, c) = (14, -15, 33)$

6. Do you observe anything about the parity of the number N of primes (including ∞) for which there is insolubility? If not, construct similar exercises and solve them until the penny drops.

7.(i) Prove your observation in (6) in the special case $a = 1$, $b = -r$, $c = -s$, where r, s are distinct primes > 2.
[Hint. Quadratic reciprocity]
(ii) [Difficult]. Prove your observation for all a, b, $c \in \mathbb{Z}$.