5

Local-global principle. Conclusion of proof

We now complete the proof of the local-global principle for conics using the theorem of the last section. We recall that we had reduced the proof to that for

$$f_1X_1^2 + f_2X_2^2 + f_3X_3^2 = 0$$

where f_1, f_2, $f_3 \in \mathbf{Z}$ and $f_1 f_2 f_3$ is square free. We assume that there are points everywhere locally and we showed that this implied certain congruences to primes p dividing $2f_1f_2f_3$.

We first define a subgroup Λ of $\mathbf{Z}^3$ by imposing congruence conditions on the components of $\mathbf{x} = (x_1, x_2, x_3)$.

First case. $p \neq 2$, $p \nmid f_1f_2f_3$, say $p \mid f_1$. We saw (end of §3) that then there is an $r_p \in \mathbf{Z}$ and that

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

We impose the condition

$$x_3 \equiv r_p x_2 \quad (p).$$

Then

$$\begin{aligned} F(\mathbf{x}) &= f_1x_1^2 + f_2x_2^2 + f_3x_3^2 \\ &\equiv (f_2 + r_p^2 f_3)x_2^2 \\ &\equiv 0 \quad (p). \end{aligned}$$

Second case. $p = 2$, $2 \nmid f_1f_2f_3$. Then without loss of generality

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

We impose the conditions

$$\left.\begin{array}{ll} x_1 \equiv 0 & (2) \\ x_2 \equiv x_3 & (2) \end{array}\right\},$$

which imply

$$F(\mathbf{x}) \equiv 0 \quad (4).$$

Third case. $p = 2$, $2 \mid f_1 f_2 f_3$, say $2 \mid f_1$. Then

$$s^2 f_1 + f_2 + f_3 \equiv 0 \quad (8),$$

where $s = 0$ or 1. We impose the conditions

$$\left.\begin{array}{ll} x_2 \equiv x_3 & (4) \\ x_1 \equiv s x_3 & (2) \end{array}\right\},$$

which imply

$$F(\mathbf{x}) \equiv 0 \quad (8).$$

To sum up. The group Λ is of index m (say) $= 4|f_1 f_2 f_3|$ in $\mathbf{Z}^3$, where throughout this section $|\,|$ is the absolute value. Further,

$$F(\mathbf{x}) \equiv 0 \qquad (4\,|f_1 f_2 f_3|)$$

for $\mathbf{x} \in \Lambda$.

We apply the theorem of the previous section to Λ and the convex symmetric set

$$\mathcal{C} : |f_1|x_1^2 + |f_2|x_2^2 + |f_3|x_3^2 < 4|f_1 f_2 f_3|.$$

School geometry shows that

$$\begin{aligned} V(\mathcal{C}) &= (\pi/3).2^3.|4 f_1 f_2 f_3| \\ &> 2^3|4 f_1 f_2 f_3| \\ &= m. \end{aligned}$$

Hence there is an $\mathbf{c} \neq \mathbf{0}$ in $\Lambda \cap \mathcal{C}$. For this $\mathbf{x}$ we have

$$F(\mathbf{x}) \equiv 0 \quad (4|f_1 f_2 f_3|)$$

and

$$\begin{aligned} |F(\mathbf{x})| &\leq |f_1|x_1^2 + |f_2|x_2^2 + |f_3|x_3^2 \\ &< 4|f_1 f_2 f_3|; \end{aligned}$$

so

$$F(\mathbf{x}) = 0,$$

as required.

We conclude with some remarks.

Remark 1. We have not merely shown that there is a solution of $F(\mathbf{x}) = 0$, but we have found that there is one in a certain ellipsoid. This facilitates the search in explicitly given cases.

Remark 2. We have made no use of the condition of solubility in $\mathbb{Q}_p$ for $p \nmid 2f_1f_2f_3$. In fact this condition tells us nothing [cf. §3, Exercises 2, 3]. It is left to the reader to check that for any f_1, f_2, f_3 and p with $p \nmid 2f_1f_2f_3$ there is always a point defined over $\mathbb{Q}_p$ on

$$f_1X_1^2 + f_2X_2^2 + f_3X_3^2 = 0.$$

Remark 3. We have also nowhere used that there is local solubility for $\mathbb{Q}_\infty = \mathbb{R}$.

Hence solubility at $\mathbb{Q}_\infty$ is implied by solubility at all the $\mathbb{Q}_p$ $(p \neq \infty)$. This phenomenon is connected with quadratic reciprocity. In fact for any conic over $\mathbb{Q}$, the number of p (including ∞) for which there is not a point over $\mathbb{Q}_p$ is always even [cf. §3, Exercises 6,7]. See a book on quadratic forms (such as the author's).

§5. Exercises

1. Let

$$F(X,Y,Z) = 5X^2 + 3Y^2 + 8Z^2 + 6(YZ + ZX + XY).$$

Find rational integers x, y, z not all divisible by 13, such that

$$F(x,y,z) \equiv 0 \pmod{13^2}.$$

[*Hint.* cf. Hensel's Lemma 2 of §10.]

2. Let

$$F(X,Y,Z) = 7X^2 + 3Y^2 - 2Z^2 + 4YZ + 6ZX + 2XY.$$

Find rational integers x, y, z not all divisible by 17 such that

$$F(x,y,z) \equiv 0 \pmod{17^3}.$$