2

p-adic numbers

Most of the familiar properties of the ordinary absolute value on the real or complex fields are consequences of the following three:

(i) $|r| \geq 0$, with equality precisely for $r = 0$.
(ii) $|rs| = |r||s|$.
(iii) $|r + s| \leq |r| + |s|$.

A real-valued function $|.|$ on a field k is said to be a *valuation* if it satisfies (i), (ii) (iii). Since $(-1)^2 = 1$, properties (i)-(iii) imply that $|-1| = 1$, $|-r| = |r|$ (all r).

The rational field $\mathbf{Q}$ has other valuations than the absolute value. Let p be a fixed prime. Any rational $r \neq 0$ can be put in the shape

$$r = p^{\rho}u/v, \ \rho \in \mathbf{Z}, \ u, \ v \in \mathbf{Z}, \ p \nmid u, \ p \nmid v.$$

We define

$$|r|_p = p^{-\rho}$$

and

$$|0|_p = 0.$$

This definition clearly satisfies (i), (ii) above. Let

$$s = p^{\sigma}m/n \qquad m, \ n \in \mathbf{Z}, \ p \nmid m, \ p \nmid n,$$

so

$$|s|_p = p^{-\sigma},$$

where without loss of generality

$$\sigma \geq \rho, \text{ i.e. } |s|_p \leq |r|_p.$$

Then

$$r + s = p^{\rho}(un + p^{\sigma-\rho}mv)/vn.$$

Here $p \nmid vn$. The numerator $un + p^{\sigma-\rho}mv$ is an integer, but, at least for for $\rho = \sigma$, it may be divisible by p. Hence

$$|r + s|_p \leq p^{-\rho},$$

that is

(iii*) $|r + s|_p \leq \max\{|r|_p, |s|_p\}$.

Clearly (iii*) implies (iii), so $|\ |_p$ is a valuation. We call it the *p-adic valuation*. The inequality (iii*) is called the *ultrametric inequality*, since (iii), the *triangle inequality*, expresses the fact that $|r - s|$ is a metric. A valuation which satisfies the ultrametric inequality is said to be *non-archimedean*.

We can transfer familiar terminology from the ordinary absolute value to the p-adic case. For example, we say that a sequence $\{a_n\}$, $n = 1, 2, \ldots$ is a *fundamental sequence* if for any $\varepsilon > 0$ there is an $n_0\ (\varepsilon)$ such that

$$|a_m - a_n|_p < \varepsilon \qquad \text{whenever} \qquad m, n \geq n_0\ (\varepsilon).$$

The sequence $\{a_n\}$ *converges* to b if

$$|a_n - b|_p < \varepsilon \qquad (\text{all } n \geq n_0\ (\varepsilon)).$$

For example let

$$p = 5$$

and consider the sequence

$$\{a_n\}: \quad 3, \quad 33, \quad 333, \quad 3333, \quad \ldots .$$

Then

$$a_m \equiv a_n \qquad \bmod 5^n \qquad (m \geq n)$$

i.e.

$$|a_m - a_n|_5 \leq 5^{-n} \qquad (m \geq n).$$

Hence $\{a_n\}$ is a fundamental sequence. Indeed it is a convergent sequence, since

$$3a_n = 99\ldots99 \equiv -1(5^n),$$

i.e.

$$|3a_n + 1|_5 \leq 5^{-n}$$

and so

$$a_n \ \to -1/3$$

5-adically.

As the above example shows, the main difficulties with the p-adic valuation are psychological: something is p-adically small if it is divisible by a high power of p. Not every p-adic fundamental sequence is convergent. Let us take $p = 5$ again. Then we construct a sequence of $a_n \in \mathbf{Z}$ such that

$$a_n^2 + 1 \equiv 0 \ (5^n)$$

and

$$a_{n+1} \equiv a_n \ (5^n).$$

We start with $a_1 = 2$. Suppose that we already have a_n for some n and put $a_{n+1} = a_n + b5^n$, where $b \in \mathbf{Z}$ is to be determined. We require

$$(a_n + b5^n)^2 + 1 \equiv 0 \ (5^{n+1}),$$

that is

$$2a_n b + c \equiv 0 \ (5), \qquad (*)$$

where we already have

$$c = (a_n^2 + 1)/5^n \in \mathbf{Z}.$$

Clearly $5 \nmid a_n$ and so we can solve the congruence $(*)$ for the unknown b.

The sequence $\{a_n\}$ just constructed is a 5-adic fundamental sequence since

$$|a_m - a_n|_5 \leq 5^{-n} \qquad (m \geq n).$$

Suppose, if possible, that a_n tends 5-adically to some $e \in \mathbf{Q}$. Then

$$a_n^2 + 1 \to e^2 + 1.$$

On the other hand, by our construction,

$$a_n^2 + 1 \to 0.$$

Hence $e^2 + 1 = 0$; a contradiction.

Just as the real numbers are constructed by completing the rationals with respect to the ordinary absolute value, so the rationals can be completed with respect to $|\ |_p$ to give the field $\mathbf{Q}_p$ of *p-adic numbers*. In fact the process can be simplified because $|\ |_p$ is non-archimedean. For the reader who is unfamiliar with this way of constructing the reals, we sketch a construction of $\mathbf{Q}_p$ at the end of this section.

We say that a field K is *complete* with respect to a valuation $|.|$ if every fundamental sequence is convergent. A field K with valuation $||.||$ is said to be the *completion* of the field k with valuation $|.|$ if there is an injection

$$\lambda : k \to K$$

which preserves the valuation:

$$||\lambda a|| = |a| \qquad (a \in k)$$

and such that

(i) K is complete with respect to $||.||$

(ii) K is the closure of λk with respect to the topology induced by $||.||$ (K is not "too large").

The completion always exists and is unique (up to a unique isomorphism). We henceforth identify k with λk and $|.|$ with $||.||$, so regard k as a subfield of K.

We now discuss the structure of the p-adic field $\mathbf{Q}_p$ with its valuation $|\ |_p$.

We note that

$$|a+b|_p = |a|_p \qquad \text{if} \qquad |b|_p < |a|_p.$$

For by (iii*) $|a+b|_p \leq |a|_p$ and, since $a = (a+b)+(-b)$, we have a contradiction if $|a+b|_p < |a|_p$. It follows that the set of values taken by $|\ |_p$ on $\mathbf{Q}_p$ is precisely the same as the set for $\mathbf{Q}$. Indeed if $\alpha \in \mathbf{Q}_p$, $\alpha \neq 0$ then by (ii) of the definition of the completion, there is an $a \in \mathbf{Q}$ with $|a-\alpha|_p < |\alpha|_p$, so $|\alpha|_p = |a|_p$.

The set of $\alpha \in \mathbf{Q}_p$ with $|\alpha| \leq 1$ is called the set of *p-adic integers* $\mathbf{Z}_p$. Because $|\ |_p$ is non-archimedean, $\mathbf{Z}_p$ is a ring:

$$|\alpha|_p,\ |\beta|_p \leq 1 \Rightarrow |\alpha\beta|_p \leq 1,\ |\alpha+\beta|_p \leq 1.$$

A rational number b is in $\mathbf{Z}_p$ precisely when it has the form $b = u/v$, where $u, v \in \mathbf{Z}$, $p \nmid v$.

The numbers $\varepsilon \in \mathbf{Q}_p$ with $|\varepsilon| = 1$ are the *p-adic units*. From what was said about the values taken by $|.|_p$ on $\mathbf{Q}_p$, every $\beta \neq 0$ in $\mathbf{Q}_p$ is of the shape $\beta = p^n\varepsilon$, where $n \in \mathbf{Z}$ and ε is a unit. The units are just the elements ε of $\mathbf{Q}_p$ such that $\varepsilon \in \mathbf{Z}_p$, $\varepsilon^{-1} \in \mathbf{Z}_p$.

As we have already noted, elementary analysis continues to hold in $\mathbf{Q}_p$, but can be simpler; as the following lemma shows.

Lemma 1. *In $\mathbf{Q}_p$ the series $\sum_0^\infty \beta_n$ converges if and only if $\beta_n \to 0$.*

Proof. By saying that the sum converges, we mean, of course, that the partial sums $\sum_0^N$ tend to a limit.

That convergence implies $\beta_n \to 0$ is true even in real analysis. To

prove the opposite implication, we note that

$$|\sum_0^N - \sum_0^M|_p = |\sum_{M+1}^N \beta_n|_p$$
$$\leq \max_{M<n\leq N} |\beta_n|_p$$

by an obvious extension of the ultrametric inequality (iii*) to several summands. Hence $\left\{\sum_0^N \beta_n\right\}$ is a fundamental sequence, so tending to a limit by the completeness of $\mathbf{Q}_p$.

We are now in a position to give an explicit description of $\mathbf{Z}_p$. We write

$$\mathcal{A} = \{0, 1, \ldots, p-1\}.$$

Lemma 2. *The elements of $\mathbf{Z}_p$ are precisely the sums*

$$\alpha = \sum_0^\infty a_n p^n,$$

where

$$a_n \in \mathcal{A} \qquad (\text{all } n).$$

Proof. By the preceeding lemma, the infinite sum converges, and its value is clearly in $\mathbf{Z}_p$.

Now let $\alpha \in \mathbf{Z}_p$ be given. There is a $b \in \mathbf{Q}$ such that $|b - \alpha|_p < 1$, and it is easy to prove that there is precisely one $a_0 \in \mathcal{A}$ such that $|a_0 - b|_p < 1$. Then

$$\alpha = a_0 + p\alpha_1$$

where $|\alpha_1| \leq 1$, i.e. $\alpha_1 \in \mathbf{Z}_p$. Proceeding inductively, we get

$$\alpha = a_0 + a_1 p + \ldots + a_N p^N + \alpha_N p^{N+1}$$

with $\alpha_N \in \mathbf{Z}_p$.

For the final result we must distinguish between $p = 2$ and $p \neq 2$.

Lemma 3 ($p \neq 2$). *Let $\alpha \in \mathbf{Q}_p$ be a unit. A necessary and sufficient condition that $\alpha = \beta^2$ for some $\beta \in \mathbf{Q}_p$ in that there is some $\gamma \in \mathbf{Q}_p$ with*

$$|\alpha - \gamma^2|_p < 1.$$

Proof. Necessity is obvious. We have already in effect given a proof in the special case $p = 5$, $\alpha = -1$. That in the general case is similar: one

constructs inductively $\beta_1 = \gamma, \beta_2, \beta_3, \ldots$ such that

$$|\beta_n^2 - \alpha| \leq p^{-n}$$

$$|\beta_{n+1} - \beta_n| \leq p^{-n}$$

If we already have β_n, we take $\beta_{n+1} = \beta_n + \delta$, so

$$\beta_{n+1}^2 = \beta_n^2 + 2\beta_n\delta + \delta^2$$

and it is enough to take

$$\delta = (\alpha - \beta_n^2)/2\beta_n.$$

This lemma ceases to hold for $p = 2$ (consider $\alpha = 5$, $\beta = 1$). We have

Lemma 4 ($p = 2$). *Let $\alpha \in \mathbf{Q}_2$ be a unit. A necessary and sufficient condition that $\alpha = \beta^2$ for some $\beta \in \mathbf{Q}_2$ is that $|\alpha - 1| \leq 2^{-3}$.*

Proof. Here again, the necessity is obvious. For sufficiency we construct a sequence $\beta_1 = 1, \beta_2, \beta_3, \ldots$ as in the previous proof. The details are left to the reader.

We conclude this section by the promised sketch of the construction of $\mathbf{Q}_p$.

Denote by $\mathfrak{F}$ the set of fundamental sequences $\{a_n\}$ for $|\ |_p$, where $a_n \in \mathbf{Q}$. Then $\mathfrak{F}$ is a ring under componentwise addition and multiplication.

$$\{a_n\} + \{b_n\} = \{a_n + b_n\} : \{a_n\}\{b_n\} = \{a_n b_n\}.$$

A sequence $\{a_n\}$ is a null sequence if $a_n \to 0$ (p-adically). The set $\mathfrak{N}$ of null-sequences is clearly an ideal in $\mathfrak{F}$.

Let $\{a_n\} \in \mathfrak{F}$ but $\{a_n\} \notin \mathfrak{N}$. Then it is easy to see that there is at least one N such that $|a_N - a_n| < |a_N|_p$ for all $n > N$. Then $|a_n|_p = |a_N|_p$ for all $n \geq N$. We write $|\{a_n\}|_p = |a_N|_p$. If $a_n \neq 0$ for all n, it is now **easy to deduce that** $\{a_n^{-1}\} \in \mathfrak{F}$.

We show that $\mathfrak{N}$ is a maximal ideal in $\mathfrak{F}$. For, if not, let $\mathfrak{M}$ be a strictly bigger ideal than $\mathfrak{N}$. It must contain an $\{a_n\} \notin \mathfrak{N}$. Then only finitely many of the a_n can be 0, and replacing them by (say) 1 merely adds an element of $\mathfrak{N}$. Hence we can suppose that $a_n \neq 0$ for all n. Then $\{a_n^{-1}\} \in \mathfrak{F}$, and so $\{a_n^{-1}\}\{a_n\} \in \mathfrak{M}$. Hence we should have $\mathfrak{M} = \mathfrak{F}$, a contradiction. We conclude that $\mathfrak{N}$ is maximal, and thus $\mathfrak{F}/\mathfrak{N}$ is a field.

The field $\mathbf{Q}$ is mapped into $\mathfrak{F}/\mathfrak{N}$ by

$$r \to \{r\} \in \mathfrak{F}.$$

The function $|\{a_n\}|$ on $\mathfrak{F}$ induces a function on $\mathfrak{F}/\mathfrak{N}$ which is easily seen to be a valuation and to coincide with $|\ |_p$ on the image of $\mathbf{Q}$.

Finally, it is not difficult to check that $\mathfrak{F}/\mathfrak{N}$ is itself complete by a diagonal argument on a sequence of elements of $\mathfrak{F}$.

§2. Exercises

1. For each of the sets of p, m, r given, either find an $x \in \mathbf{Z}$ such that

$$|r - x|_p \leq p^{-m},$$

or show that no such x exists.

(i) $p = 257$, $r = 1/2$, $m = 1$;
(ii) $p = 3$, $r = 7/8$, $m = 2$;
(iii) $p = 3$, $r = 7/8$, $m = 7$;
(iv) $p = 3$, $r = 5/6$, $m = 9$;
(v) $p = 5$, $r = 1/4$, $m = 4$.

2. Construct further examples along the lines of Exercise 1 until the whole business seems trivial.

3. For given p, m, r either find an $x \in \mathbf{Z}$ such that

$$|r - x^2|_p \leq p^{-m}$$

or show that no such x exists.

(i) $p = 5$, $r = -1$, $m = 4$;
(ii) $p = 5$, $r = 10$, $m = 3$;
(iii) $p = 13$, $r = -4$, $m = 3$;
(iv) $p = 2$, $r = -7$, $m = 6$;
(v) $p = 7$, $r = -14$, $m = 4$;
(vi) $p = 7$, $r = 6$, $m = 3$;
(vii) $p = 7$, $r = 1/2$, $m = 3$.

4. As Exercise 2.

5. Let $p > 0$ be prime, $p \equiv 2\ (3)$. For any integer a, $p \nmid a$, show that there is an $x \in \mathbf{Z}_p$ with $x^3 = a$.

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.

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 $f_1f_2f_3$. After a finite number of steps we are reduced to the case when $f_1f_2f_3$ is square free. We have thus proved the

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

$$F(\mathbf{X}) = f_1X_1^2 + f_2X_2^2 + f_3X_3^2 = 0,$$

where $f_j \in \mathbf{Z}$ *and* $f_1f_2f_3$ *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. $p \neq 2$, $p \mid f_1f_2f_3$. Without loss of generality $p \mid f_1$, so $p \nmid f_2$, $p \nmid f_3$. Then $|f_1a_1^2|_p < 1$. Suppose, if possible that $|a_2|_p < 1$. Then

$$|f_3a_3^2|_p = |f_1a_1^2 + f_2a_2^2|_p < 1$$

and $|a_3|_p < 1$. Now

$$|f_1a_1^2|_p = |f_2a_2^2 + f_3a_3^2|_p \leq p^{-2}$$

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

$$|f_2a_2^2 + f_3a_3^2|_p < 1.$$

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

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

Second case. $p = 2$, $2 \nmid f_1f_2f_3$. 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. $p = 2$, $2 \mid f_1f_2f_3$, 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 $b, c \in \mathbf{Z}$, $p \nmid b$. Show that $bx^2 + c$ takes precisely $\frac{1}{2}(p+1)$ distinct values p for $x \in \mathbf{Z}$. (ii) Suppose that, further, $a \in \mathbf{Z}$, $p \nmid a$. Show that there are $x, y \in \mathbf{Z}$ such that $bx^2 + c \equiv ay^2 \ (p)$.

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

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

4. Let $a, b, c \in \mathbf{Z}$, $2 \nmid abc$. Show that a necessary and sufficient condition that the only solution in $\mathbf{Q}_2$ 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 $\mathbf{Q}_p$ 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 $a, b, c \in \mathbf{Z}$.

4

Geometry of numbers

At this stage we require a tool from the Geometry of Numbers, which we shall develop from scratch.

A generalization of the pigeon-hole principle (Schubfachprinzip) says that if we have N things to file in H holes and $N > mH$ for an integer m, then at least one of the holes will contain $\geq (m+1)$ things. We start with a continuous analogue.

Let $\mathbf{R}^n$ denote the vector space of real n-tuples $\mathbf{r} = (r_1, \ldots, r_n)$. It contains the group $\mathbf{Z}^n$ of $\mathbf{r}$ for which $r_j \in \mathbf{Z}$ (all j). By the volume $V(\mathcal{S})$ of a set $\mathcal{S} \subset \mathbf{R}^n$ we shall mean its Lebesgue measure, but in the applications we will be concerned only with very simple-minded $\mathcal{S}$.

Lemma 1. *Let $m > 0$ be an integer and let $\mathcal{S} \subset \mathbf{R}^n$ with*

$$V(\mathcal{S}) > m.$$

Then there are $m+1$ distinct points $\mathbf{s}_0, \ldots, \mathbf{s}_m$ of S such that

$$\mathbf{s}_i - \mathbf{s}_j \in \mathbf{Z}^n \qquad (0 \leq i,\ j \leq m).$$

Proof. Let $\mathcal{W} \subset \mathbf{R}^n$ be the "unit cube" of points $\mathbf{w}$ with

$$0 \leq w_j < 1 \qquad (1 \leq j \leq n).$$

Then every $\mathbf{x} \in \mathbf{R}^n$ is uniquely of the shape

$$\mathbf{x} = \mathbf{w} + \mathbf{z},$$

where $\mathbf{z} \in \mathbf{Z}^n$. Let $\psi(\mathbf{x})$ be the characteristic function of $\mathcal{S}$ ($= 1$ if $\mathbf{x} \in \mathcal{S}$,

$= 0$ otherwise). Then

$$m < V(\mathcal{S}) = \int_{\mathbf{R}^n} \psi(\mathbf{x})d\mathbf{x}$$

$$= \int_{\mathcal{W}} \left(\sum_{\mathbf{z}\in\mathbf{Z}^n} \psi(\mathbf{w}+\mathbf{z}) \right) d\mathbf{w}.$$

Since $V(\mathcal{W}) = 1$, there must be some $\mathbf{w}_0 \in \mathcal{W}$ such that

$$\sum_{\mathbf{z}\in\mathbf{Z}^n} \psi(\mathbf{w}_0+\mathbf{z}) > m,$$

$$\text{so} \quad \geq m+1.$$

We may now take for the $\mathbf{s}_j$ the $\mathbf{w}_0 + \mathbf{z}$ for which $\psi(\mathbf{w}_0+\mathbf{z}) > 0$.

The set $\mathcal{S}$ is said to be *symmetric* (about the origin) if $-\mathbf{x} \in \mathcal{S}$ whenever $\mathbf{x} \in \mathcal{S}$. It is *convex* if whenever $\mathbf{x}, \mathbf{y} \in \mathcal{S}$, then the whole line-segment

$$\lambda\mathbf{x} + (1-\lambda)\mathbf{y} \in \mathcal{S} \qquad (0 \leq \lambda \leq 1)$$

joining them is in $\mathcal{S}$. In particular, the mid-point $\frac{1}{2}(\mathbf{x}+\mathbf{y})$ is in $\mathcal{S}$.

Theorem 1. *Let Λ be a subgroup of $\mathbf{Z}^n$ of index m. Let $\mathcal{C} \subset \mathbf{R}^n$ be a symmetric convex set of volume*

$$V(\mathcal{C}) > 2^n m.$$

Then $\mathcal{C}$ and Λ have a common point other than $\mathbf{0} = (0,\ldots,0)$.

Proof. Let $\mathcal{S} = \frac{1}{2}\mathcal{C}$ be the set of points $\frac{1}{2}\mathbf{c}$, $\mathbf{c} \in \mathcal{C}$. Then

$$V(\tfrac{1}{2}\mathcal{C}) = 2^{-n}V(\mathcal{C}) > m.$$

By Lemma 1, there are $m+1$ distinct points $\mathbf{c}_0, \ldots, \mathbf{c}_m \in \mathcal{C}$ such that

$$\tfrac{1}{2}\mathbf{c}_i - \tfrac{1}{2}\mathbf{c}_j \in \mathbf{Z}^n . \quad (0 \leq i,\ j \leq m).$$

There are $m+1$ points

$$\tfrac{1}{2}\mathbf{c}_i - \tfrac{1}{2}\mathbf{c}_0 \qquad (0 \leq i \leq m)$$

and m cosets of $\mathbf{Z}^n$ modulo Λ. By the pigeon hole principle, two must be in the same coset, that is there are i, j with $i \neq j$ such that

$$\tfrac{1}{2}\mathbf{c}_i - \tfrac{1}{2}\mathbf{c}_j \in \Lambda.$$

Now $-\mathbf{c}_j \in \mathcal{C}$ by symmetry; and so

$$\tfrac{1}{2}\mathbf{c}_i - \tfrac{1}{2}\mathbf{c}_j = \tfrac{1}{2}\mathbf{c}_i + \tfrac{1}{2}(-\mathbf{c}_j) \in \mathcal{C}$$

by convexity.

Note. Lemma 1 and Theorem 1 with $m = 1$ are due to Blichfeldt and Minkowski respectively. The generalizations to $m > 1$ are by van der Corput.

As a foretaste of the flavour of the application in the next section, we give

Lemma 2. *Let N be a positive integer. Suppose that there is an $l \in \mathbf{Z}$ such that*

$$l^2 \equiv -1 \ (N).$$

Then $N = u^2 + v^2$ for some $u, v \in \mathbf{Z}$.

Proof. We take $n = 2$ and denote the co-ordinates by x, y. For $\mathcal{C}$ we take the open disc

$$x^2 + y^2 < 2m$$

of volume (= area)

$$V(\mathcal{C}) = 2\pi m > 2^2 m.$$

The subgroup Λ of $\mathbf{Z}^2$ is given by

$$x, y \in \mathbf{Z}, \qquad y \equiv lx \ \ (m).$$

It is clearly of index m. Hence by the Theorem there is

$$(0,0) \neq (u,v) \in \Lambda \cap \mathcal{C}.$$

Then

$$0 < u^2 + v^2 < 2m$$

and

$$u^2 + v^2 \equiv u^2(1 + l^2) \equiv 0 \ \ (m).$$

Hence $u^2 + v^2 = m$, as required.

We note, in passing, that the condition of the lemma is certainly satisfied for primes p with $p \equiv 1 \ (4)$.

§4. Exercises

1. Let $m \in \mathbf{Z}$, $m > 1$ and suppose that there is some $f \in \mathbf{Z}$ such that $f^2 + f + 1 \equiv 0 \ (m)$. Show that $m = u^2 + uv + v^2$ for some $u, v \in \mathbf{Z}$.

2. Find a prime $p > 0$ for which there is an $f \in \mathbf{Z}$ such that

$$1 + 5f^2 \equiv 0 \ (p)$$

but p is not of the shape $u^2 + 5v^2$ $(u, v \in \mathbf{Z})$.

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 $f_1f_2f_3$ 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

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

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

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

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 $\mathbf{Q}_p$ 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 $\mathbf{Q}_p$ 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 $\mathbf{Q}_\infty = \mathbf{R}$.

Hence solubility at $\mathbf{Q}_\infty$ is implied by solubility at all the $\mathbf{Q}_p$ ($p \neq \infty$). This phenomenon is connected with quadratic reciprocity. In fact for any conic over $\mathbf{Q}$, the number of p (including ∞) for which there is not a point over $\mathbf{Q}_p$ 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

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