ANNALS OF MATHEMATICS
Vol. 41, No. 1, January, 1940

ON A GEOMETRICAL REPRESENTATION OF p-ADIC NUMBERS

BY KURT MAHLER

(Received December 30, 1938)

Let ζ be a real irrational number,

$$\zeta = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \cdots$$

its simple continued fraction, and

$$\frac{p_0}{q_0} = \frac{a_0}{1}, \qquad \frac{p_1}{q_1} = \frac{a_0 a_1 + 1}{a_1}, \qquad \frac{p_2}{q_2}, \cdots$$

the sequence of its approximations. The following theorems have been proved:

THEOREM OF LAGRANGE:[1] *If p/q is a rational number, such that*

$$\left|\zeta - \frac{p}{q}\right| \leqq \left|\zeta - \frac{p_n}{q_n}\right|$$

for a certain index $n \geqq 1$, then $|q| \geqq q_n$, with equality if and only if $\frac{p}{q} = \frac{p_n}{q_n}$.

THEOREM OF HURWITZ-BOREL:[2] *For at least one of any three consecutive indices n*

$$\left|\zeta - \frac{p_n}{q_n}\right| < \frac{1}{\sqrt{5}}\, q_n^{-2},$$

but to every $\epsilon > 0$, there is an irrational number ζ, such that

$$\left|\zeta - \frac{p_n}{q_n}\right| \geqq \left(\frac{1}{\sqrt{5}} - \epsilon\right) q_n^{-2}$$

for all sufficiently large n.

THEOREM OF KHINTCHINE:[3] *There are arbitrarily large positive integers t, for which the inequalities*

$$\left|\zeta - \frac{p}{q}\right| < \frac{1}{t\,|q|}, \qquad 0 < |q| \leqq \frac{t}{2}$$

have no solution in integers p, q.

---

[1] O. Perron, *Die Lehre von den Kettenbrüchen*, Leipzig-Berlin 1929, §15.

[2] l. c. 1, §14.

[3] J. F. Koksma, *Diophantische Approximationen*, Berlin 1936, p. 36 f.

THEOREM OF TCHEBYCHEFF:[4] *If ζ is an irrational, ϑ an arbitrary real number, then there are arbitrarily large positive integers t, for which the inequalities*

$$|q\zeta - p - \vartheta| \leqq \frac{1}{t}, \qquad |q| \leqq \frac{t}{2}$$

have an integer solution p, q.

(Though the statement of the last two theorems does not mention continued fractions, their proof is much simpler if these are used.)

In the present paper, I derive analogous results for P-adic numbers, when P is an arbitrary positive prime number; see the Theorems 17–26 in Part II. For this purpose it is necessary to develop a P-adic algorithm similar to that of the continued fractions in the real field. In two earlier papers,[5] I have previously studied and applied an algorithm of this kind; the method there was purely arithmetical and based on Minkowski's Theorem on linear forms. It had, however, some disadvantages, e.g. it did not lead to analogues to the Theorems of Hurwitz-Borel and Khintchine with good values of the constants.

For this reason, I shall use in this paper a geometrical method, by which the best approximations of a given P-adic integer ζ can always be obtained. (The restriction to P-adic integers is unimportant, since, if necessary, $1/\zeta$ instead of ζ may be considered.) This method forms something like a P-adic counterpart to Hermite's method of introduction of continuous variables in the theory of forms.[6] It is based on the following idea:

Let

$$\mathrm{T}_n = \begin{pmatrix} p_n & p_n' \\ q_n & q_n' \end{pmatrix} \qquad (n = 0, 1, 2, \ldots)$$

be an infinite sequence of integer matrices with the following properties:

(a): $$p_n q_n' - p_n' q_n = P^n.$$

(b): $$(q_n , q_n') = 1.$$

(c): All matrices $\mathrm{T}_n^{-1}\mathrm{T}_{n+1} = \Omega_{n+1}$ have integer elements.

Then it is easily verified that to every n there is an integer A_n, such that $0 \leqq A_n \leqq P^n - 1$, $p_n + q_n A_n \equiv 0 \pmod{P^n}$, $p_n' + q_n' A_n \equiv 0 \pmod{P^n}$, and such that

$$A_{n+1} \equiv A_n \pmod{P^n}.$$

There exists, therefore, a P-adic integer ζ as the P-adic limit

$$\zeta = \lim_{n \to \infty} A_n.$$

---

[4] l. c. 3, p. 76 f.

[5] *Nieuw Arch. Wiskde* (2), **18** (1934), 22–34, and *Mathematica* B (Zutphen), VII (1938), 5 p.

[6] Ch. Hermite, *Oeuvres*, vol. 1, Paris 1905, 100–163, 164–193, 200–263, and l. c. 3, p. 40 f.

This number is determined uniquely by the sequence $\{\mathrm{T}_n\}$, and it is related to its elements T_n by the inequalities

$$|p_n + q_n\zeta|_P \leqq P^{-n}, \qquad |p'_n + q'_n\zeta|_P \leqq P^{-n}$$

and the equations[7]

$$\zeta = \lim_{n\to\infty}\left(-\frac{p_n}{q_n}\right) \quad \text{or} \quad \lim_{n\to\infty}\left(-\frac{p'_n}{q'_n}\right).$$

We say that the sequence $\{\mathrm{T}_n\}$ defines ζ. Conversely, every P-adic integer can be defined by a sequence $\{\mathrm{T}_n\}$; it is sufficient to take

$$\mathrm{T}_n = \begin{pmatrix} P^n & -A_n \\ 0 & 1 \end{pmatrix} \qquad (n = 0, 1, 2, \cdots),$$

where A_n is any integer for which

$$|\zeta - A_n|_P \leqq P^{-n}.$$

Then $(A_{n+1} - A_n)/P^n$ is an integer, and therefore also all matrices

$$\mathrm{T}_n^{-1}\mathrm{T}_{n+1} = \begin{pmatrix} -P & (A_{n+1} - A_n)P^{-n} \\ 0 & -1 \end{pmatrix}$$

are integral. The three conditions (a), (b), (c) are therefore satisfied.

Let us consider two sequences $\{\mathrm{T}_n\}$ and $\{\mathrm{T}_n^*\}$ as equivalent if they define the same number ζ. This is the case if and only if to every index $n = 0, 1, 2, \cdots$ there is an element P_n of the modular group (i.e. an integer matrix of determinant 1), such that

$$\mathrm{T}_n^* = \mathrm{T}_n\mathrm{P}_n .$$

Among all equivalent sequences $\{\mathrm{T}_n\}$, which define ζ, we can choose one as the reduced sequence. This we may do, for instance, in the following way:

Let $\Phi(X, Y)$ be the distance function of an arbitrary convex domain $\Phi(X, Y) \leqq 1$ of area J in the (X, Y)-plane with center at the origin; thus

$$\Phi(0, 0) = 0, \qquad \Phi(X, Y) > 0 \quad \text{for} \quad X^2 + Y^2 > 0,$$

$$\Phi(tX, tY) = |t|\,\Phi(X, Y) \qquad \text{for real } t,$$

$$\Phi(X_1 + X_2, Y_1 + Y_2) \leqq \Phi(X_1, Y_1) + \Phi(X_2, Y_2).$$

With every element $\mathrm{T}_n = \begin{pmatrix} p_n & p'_n \\ q_n & q'_n \end{pmatrix}$ of $\{\mathrm{T}_n\}$ we form the new convex function

$$\Phi_n(X, Y) = \Phi(p_nX + p'_nY, q_nX + q'_nY);$$

[7] One of these limits may be different from ζ.

the domain $\Phi_n(X, Y) \leqq 1$ is again convex with center at the origin, and its area is $P^{-n}J$. Suppose now that for every $n = 0, 1, 2, \cdots$ the function $\Phi_n(X, Y)$ satisfies the inequalities

(d): $$\Phi_n(1, 0) \leqq \Phi_n(0, 1) \leqq \Phi_n(-1, 1) \leqq \Phi_n(1, 1);$$

then we say that the sequence $\{\mathbf{T}_n\}$ is reduced. By Minkowski,[8] it follows from (d) that

(e): $$\frac{2P^n}{J} \leqq \Phi_n(1, 0)\Phi_n(0, 1) \leqq \frac{4P^n}{J}.$$

Hence in particular, for all indices n simultaneously

(f): $$|p_n + q_n\zeta|_P \leqq P^{-n}, \qquad \Phi(p_n, q_n) \leqq \frac{2P^{n/2}}{\sqrt{J}}.$$

It is not difficult to show that there is one and only one reduced sequence which defines ζ; by (f), the elements of this sequence lead to approximations $-p_n/q_n$ for ζ.—It can also be shown that if $\{\mathbf{T}_n\}$ is reduced, then every term of the allied sequence

$$\Omega_{n+1} = \mathbf{T}_n^{-1}\mathbf{T}_{n+1} \qquad (n = 0, 1, 2, \cdots)$$

belongs to a finite set of matrices, which depends only on P and on the function $\Phi(X, Y)$, but not on ζ. By means of this result, it is possible to determine indices n, for which the inequalities (f) can be improved, provided that such indices exist; it is further possible to obtain results analogous to the Theorem of Khintchine.

This is carried through in the present paper for the case in which

$$\Phi(X, Y)^2 = \mathbf{A}X^2 + 2\mathbf{B}XY + \mathbf{C}Y^2$$

is a positive definite quadratic form of determinant 1. In this case, the inequalities (e) and (f) can be improved a little. It is more important, however, that the conditions (d) now become the well known conditions for a reduced positive definite quadratic form, viz.

$$-\mathbf{A}_n \leqq 2\mathbf{B}_n < \mathbf{A}_n \leqq \mathbf{C}_n,$$

if

$$\Phi_n(X, Y)^2 = \mathbf{A}_nX^2 + 2\mathbf{B}_nXY + \mathbf{C}_nY^2.$$

Therefore, if in the usual way[9] we represent the form $\Phi_n(X, Y)$ by the point z_n in the upper half of the complex plane which satisfies the equation $\Phi_n(z, 1) = 0$, then z_n will lie in the fundamental domain F of the modular group. Hence,

---

[8] *Geometrie der Zahlen*, Leipzig-Berlin 1910, 193–196.

[9] P. Bachmann, *Quadratische Formen II*, Leipzig-Berlin 1923, p. 17 f.

as a geometrical representative of ζ, we get an infinite set of points z_n in F. Two consecutive points of this set are connected by the equation

$$(g): \qquad z_n = \frac{\alpha_{n+1} z_{n+1} + \alpha'_{n+1}}{\beta_{n+1} z_{n+1} + \beta'_{n+1}},$$

if $\Omega_{n+1} = \begin{pmatrix} \alpha_{n+1} & \alpha'_{n+1} \\ \beta_{n+1} & \beta'_{n+1} \end{pmatrix}$. As we have already remarked, the matrices Ω_{n+1} have only a finite number of possibilities independent of ζ; it is quite easy to find all these for a given prime number P. We can, therefore, study the elements of the sequence $\{z_n\}$ without specializing ζ; for instance, we can find lower bounds for $\limsup_{n\to\infty} y_n$, where $z_n = x_n + iy_n$. Since

$$| p_n + q_n\zeta |_P \leqq P^{-n}, \qquad | p'_n + q'_n\zeta |_P \leqq P^{-n}$$

and

$$\Phi(p_n, q_n)^2 = \frac{P^n}{y_n}, \qquad \Phi(p'_n, q'_n) = \frac{P^n(x_n^2 + y_n^2)}{y_n},$$

these properties of $\{z_n\}$ are equivalent to results on Diophantine approximations to ζ. We give this investigation of $\{z_n\}$ in the first part, and the applications in the second part, of the paper.

It is quite obvious that in a similar way matrices of any order may be considered; we then shall get results on the simultaneous approximations of a system of P-adic numbers. I intend to study this problem and the analogous one in the real field in a later paper.

Part I: The Representative of a P-adic Integer

1. The sequences $Z(\zeta)$ and $z(\zeta)$

Let Γ be the modular group of all substitutions

$$(1): \qquad Z = \frac{rz + r'}{qz + q'} \qquad (rq' - r'q = 1)$$

with integer coefficients and determinant 1. Two points Z and z in the complex upper half-plane H, which are related by (1) are called equivalent. As is proved in the theory of Γ, to every point Z in H there is exactly one equivalent point z in the domain F of all points $z = x + yi$, for which

$$(2): \quad -\tfrac{1}{2} \leqq x < \tfrac{1}{2}, \qquad x^2 + y^2 > 1, \quad \text{or} \quad -\tfrac{1}{2} \leqq x \leqq 0, \qquad x^2 + y^2 = 1;$$

this domain F is called the fundamental domain of Γ.—It is useful to define the *distance* between two points z_1 and z_2 in F by

$$\rho(z_1, z_2) = \min\left(| z_1 - z_2 |, | z_1 - z_2 + 1 |, | z_1 - z_2 - 1 |, \left| z_1 + \frac{1}{z_2} \right|, \left| \frac{1}{z_1} + z_2 \right| \right);$$

then the neighborhood of a point z_1 in F consists of all points z_2 in F, which are sufficiently near either to z_1 or one of the equivalent points $z_1 + 1$, $z_1 - 1$, or

$-1/z_1$. In the following considerations, λ denotes a number in F, which is fixed, but arbitrary.

Let P be a natural prime number and ζ a P-adic integer:

$$|\zeta|_P \leqq 1.$$

For every $n = 0, 1, 2, \cdots$ we define two integers A_n and a_n by

(3): $$|\zeta - A_n|_P \leqq P^{-n}, \qquad 0 \leqq A_n \leqq P^n - 1 \qquad (A_0 = 0),$$

and

(4): $$a_n = \frac{A_{n+1} - A_n}{P^n}, \quad \text{so that} \quad 0 \leqq a_n \leqq P - 1 \qquad (a_0 = A_1),$$

and

$$\zeta = \lim_{n\to\infty} A_n = a_0 + a_1 P + a_2 P^2 + \cdots.$$

Therefore ζ is known if the sequence $A(\zeta)$ of all A_n or the sequence $a(\zeta)$ of all a_n are given.

By means of $A(\zeta)$, the sequence $Z(\zeta)$ of all numbers

(5): $$Z_n = \frac{A_n + \lambda}{P^n} \qquad (Z_0 = \lambda)$$

in H is determined; obviously

$$Z_{n+1} = \frac{Z_n + a_n}{P}.$$

A second sequence $z(\zeta)$ of complex numbers z_n is obtained, if by z_n ($n = 0, 1, 2, \cdots$) we understand the number in F which is equivalent to Z_n. This sequence $z(\zeta)$ is called the representative of ζ.

2. The matrices T_n and Ω_n

Let

(6): $$Z_n = \frac{r_n z_n + r_n'}{q_n z_n + q_n'} \quad \text{or} \quad z_n = \frac{-q_n' Z_n + r_n'}{q_n Z_n - r_n} \qquad (r_n q_n' - q_n r_n' = 1)$$

be the modular substitution which connects Z_n with z_n, and put

(7): $$p_n = P^n r_n - A_n q_n, \qquad p_n' = P^n r_n' - A_n q_n'.$$

Then from (5)

(8): $$\lambda = \frac{p_n z_n + p_n'}{q_n z_n + q_n'} \quad \text{or} \quad z_n = \frac{-q_n' \lambda + p_n'}{q_n \lambda - p_n},$$

or symbolically

$$\lambda = \mathrm{T}_n z_n, \qquad z_n = \mathrm{T}_n^{-1} \lambda,$$

where $\mathbf{T}_n$ denotes the matrix

(9): $$\mathbf{T}_n = \begin{pmatrix} p_n & p_n' \\ q_n & q_n' \end{pmatrix}.$$

Since $r_n q_n' - r_n' q_n = 1$, $\mathbf{T}_n$ has the determinant

(10): $$p_n q_n' - p_n' q_n = P^n,$$

and its two lower elements q_n and q_n' are relatively prime. At least one of the q's, therefore, is not divisible by P, say q_n^* ; by p_n^* we denote the element of $\mathbf{T}_n$ above q_n^* . In particular for $n = 0$,

$$\mathbf{T}_0 = \mathbf{E} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad p_0^* = 0, \qquad q_0^* = 1,$$

since $Z_0 = \lambda$ lies in F and therefore $Z_0 = z_0$.

The sequence $\mathbf{T}(\zeta)$ of all matrices $\mathbf{T}_n$ has a number of simple properties. Obviously

$$\mathbf{T}_n = \begin{pmatrix} P^n & -A_n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} r_n & r_n' \\ q_n & q_n' \end{pmatrix}.$$

Therefore, if for $n = 0, 1, 2, \cdots$

(11): $$\Omega_{n+1} = \mathbf{T}_n^{-1} \mathbf{T}_{n+1} = \begin{pmatrix} \alpha_{n+1} & \alpha_{n+1}' \\ \beta_{n+1} & \beta_{n+1}' \end{pmatrix},$$

say, then Ω_{n+1} has the determinant

(12): $$\alpha_{n+1} \beta_{n+1}' - \alpha_{n+1}' \beta_{n+1} = P.$$

Also

$$\Omega_{n+1} = \begin{pmatrix} r_n & r_n' \\ q_n & q_n' \end{pmatrix}^{-1} \begin{pmatrix} P^n & -A_n \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} P^{n+1} & -A_{n+1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} r_{n+1} & r_{n+1}' \\ q_{n+1} & q_{n+1}' \end{pmatrix},$$

or after a simplification

$$\Omega_{n+1} = -\begin{pmatrix} r_n & r_n' \\ q_n & q_n' \end{pmatrix}^{-1} \begin{pmatrix} P & -a_n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} r_{n+1} & r_{n+1}' \\ q_{n+1} & q_{n+1}' \end{pmatrix},$$

so that all elements of Ω_{n+1} are integers. We denote the sequence of all Ω_{n+1} by $\Omega(\zeta)$. It can be determined from $\mathbf{T}(\zeta)$ by means of (11); conversely

(13): $$\mathbf{T}_0 = \mathbf{E}, \qquad \mathbf{T}_n = \Omega_1 \Omega_2 \cdots \Omega_n \quad \text{for} \quad n = 1, 2, 3, \cdots,$$

so that $\mathbf{T}(\zeta)$ follows also from $\Omega(\zeta)$. Obviously from (8) and (11)

(14): $$z_n = \Omega_{n+1} z_{n+1} = \frac{\alpha_{n+1} z_{n+1} + \alpha_{n+1}'}{\beta_{n+1} z_{n+1} + \beta_{n+1}'}, \qquad z_{n+1} = \Omega_{n+1}^{-1} z_n = \frac{-\beta_{n+1}' z_n + \alpha_{n+1}'}{\beta_{n+1} z_n - \alpha_{n+1}}.$$

Hence all Ω_{n+1} have the following important property: If $\Omega_{n+1}F$ denotes the domain of all points $z' = \Omega_{n+1}z$, where z lies in F, then F and $\Omega_{n+1}F$ have at least one common point.

3. The theorem of finiteness

From the last remark, we deduce the result:

THEOREM 1: *All terms Ω_{n+1} of the sequence $\Omega(\zeta)$ belong to a finite set $M(P)$ of integer matrices of determinant P, which depends only on P.*

PROOF: Since it is just as easy, we prove a more general result. Suppose that Q is an arbitrary positive integer; let $M(Q)$ denote the set of all integer matrices Ω of determinant Q, for which the two domains F and ΩF have at least one common point. Then we prove that $M(Q)$ is a finite set. Now every integer matrix Ω of determinant Q can be written as

$$\Omega = \mathrm{P}\Sigma,$$

where P is an element of Γ, and

$$\Sigma = \begin{pmatrix} u & v \\ 0 & w \end{pmatrix}$$

is an integer matrix, such that

$$uw = Q, \qquad u > 0, \qquad w > 0, \qquad 0 \leqq v \leqq w - 1.$$

Obviously, there are only a finite number of matrices Σ with these properties, say the matrices

$$\Sigma_h \qquad (h = 1, 2, \cdots, \sigma).$$

The transformed domains

$$\Sigma_h F$$

all lie entirely in the part of the z-plane given by

$$|x| \leqq Q, \qquad y \geqq \frac{\sqrt{3}}{2Q},$$

and therefore enter only a finite number of triangles of the modular division of the z-plane. Hence to every Σ_h there can be only a finite number of elements

$$\mathrm{P}_{hk} \qquad (k = 1, 2, \cdots, \rho_h)$$

of Γ, such that $\mathrm{P}_{hk}\Sigma_h$ belongs to $M(Q)$, and the theorem follows at once.

4. The cases $P = 2$, $P = 3$ and $P = 5$ of Theorem 1

The last proof gives a method for the actual determination of $M(Q)$ and in particular of $M(P)$. We give here the results for the smallest prime numbers P.

For this purpose we divide $M(P)$ into three subsets $M_1(P)$, $M_2(P)$ and $M_3(P)$.

An element Ω of $M(P)$ belongs to the first, second or third of these sets, according as the set of the common points of F and ΩF has positive area, or forms an arc of a curve, or consists of a single point. For $P = 2$ both $M_2(P)$ and $M_3(P)$ are empty, but this is not true for any larger prime number P.

In the following tables, the elements of $M_j(P)$ $(j = 1, 2, 3)$ are arranged in such a way that any two of them stand one above the other, if their product is equal to $\mp P\mathbf{E}$, and that they stand alone, if their square has this value. With Ω also $-\Omega$ belongs to $M_j(P)$; these two matrices lead to the same relation between points of F and therefore are not essentially different.

CASE $P = 2$:

$M(2) = M_1(2)$ has 26 elements:

$$\mp\begin{pmatrix} 0 & 2 \\ -1 & 0 \end{pmatrix}, \quad \mp\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mp\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \quad \mp\begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix}, \quad \mp\begin{pmatrix} 0 & 2 \\ -1 & 1 \end{pmatrix},$$

$$\mp\begin{pmatrix} -1 & 0 \\ 0 & -2 \end{pmatrix}, \quad \mp\begin{pmatrix} -1 & 1 \\ 0 & -2 \end{pmatrix}, \quad \mp\begin{pmatrix} -1 & -1 \\ 0 & -2 \end{pmatrix}, \quad \mp\begin{pmatrix} -1 & 2 \\ -1 & 0 \end{pmatrix},$$

$$\mp\begin{pmatrix} 0 & 2 \\ -1 & -1 \end{pmatrix}, \quad \mp\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix},$$

$$\mp\begin{pmatrix} 1 & 2 \\ -1 & 0 \end{pmatrix}, \quad \mp\begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}.$$

CASE $P = 3$:

$M_1(3)$ has 26 elements:

$$\mp\begin{pmatrix} 0 & 3 \\ -1 & 0 \end{pmatrix}, \quad \mp\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mp\begin{pmatrix} 3 & 1 \\ 0 & 1 \end{pmatrix}, \quad \mp\begin{pmatrix} 3 & -1 \\ 0 & 1 \end{pmatrix}, \quad \mp\begin{pmatrix} 0 & 3 \\ -1 & 1 \end{pmatrix},$$

$$\mp\begin{pmatrix} -1 & 0 \\ 0 & -3 \end{pmatrix}, \quad \mp\begin{pmatrix} -1 & 1 \\ 0 & -3 \end{pmatrix}, \quad \mp\begin{pmatrix} -1 & -1 \\ 0 & -3 \end{pmatrix}, \quad \mp\begin{pmatrix} -1 & 3 \\ -1 & 0 \end{pmatrix},$$

$$\mp\begin{pmatrix} 0 & 3 \\ -1 & -1 \end{pmatrix}, \quad \mp\begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix},$$

$$\mp\begin{pmatrix} 1 & 3 \\ -1 & 0 \end{pmatrix}, \quad \mp\begin{pmatrix} -1 & 2 \\ -1 & -1 \end{pmatrix};$$

$M_2(3)$ has 4 elements:

$$\mp\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix},$$

$$\mp\begin{pmatrix} -1 & 1 \\ -1 & -2 \end{pmatrix};$$

$M_3(3)$ has 6 elements:

$$\mp\begin{pmatrix}-1 & -2\\ 2 & 1\end{pmatrix}, \quad \mp\begin{pmatrix}0 & -3\\ 1 & 2\end{pmatrix}, \quad \mp\begin{pmatrix}-2 & -3\\ 1 & 0\end{pmatrix}.$$

CASE $P = 5$:

$M_1(5)$ has 58 elements:

$$\mp\begin{pmatrix}0 & 5\\ -1 & 0\end{pmatrix}, \quad \mp\begin{pmatrix}5 & 0\\ 0 & 1\end{pmatrix}, \quad \mp\begin{pmatrix}5 & 1\\ 0 & 1\end{pmatrix}, \quad \mp\begin{pmatrix}5 & -1\\ 0 & 1\end{pmatrix}, \quad \mp\begin{pmatrix}5 & 2\\ 0 & 1\end{pmatrix},$$

$$\mp\begin{pmatrix}-1 & 0\\ 0 & -5\end{pmatrix}, \quad \mp\begin{pmatrix}-1 & 1\\ 0 & -5\end{pmatrix}, \quad \mp\begin{pmatrix}-1 & -1\\ 0 & -5\end{pmatrix}, \quad \mp\begin{pmatrix}-1 & 2\\ 0 & -5\end{pmatrix},$$

$$\mp\begin{pmatrix}5 & -2\\ 0 & 1\end{pmatrix}, \quad \mp\begin{pmatrix}1 & -5\\ 1 & 0\end{pmatrix}, \quad \mp\begin{pmatrix}2 & -5\\ 1 & 0\end{pmatrix}, \quad \mp\begin{pmatrix}0 & -5\\ 1 & 1\end{pmatrix},$$

$$\mp\begin{pmatrix}-1 & -2\\ 0 & -5\end{pmatrix}, \quad \mp\begin{pmatrix}0 & -5\\ 1 & -1\end{pmatrix}, \quad \mp\begin{pmatrix}0 & -5\\ 1 & -2\end{pmatrix}, \quad \mp\begin{pmatrix}-1 & -5\\ 1 & 0\end{pmatrix},$$

$$\mp\begin{pmatrix}0 & -5\\ 1 & 2\end{pmatrix}, \quad \mp\begin{pmatrix}1 & -4\\ 1 & 1\end{pmatrix}, \quad \mp\begin{pmatrix}1 & -3\\ 1 & 2\end{pmatrix}, \quad \mp\begin{pmatrix}1 & -2\\ 2 & 1\end{pmatrix},$$

$$\mp\begin{pmatrix}-2 & -5\\ 1 & 0\end{pmatrix}, \quad \mp\begin{pmatrix}-1 & -4\\ 1 & -1\end{pmatrix}, \quad \mp\begin{pmatrix}-2 & -3\\ 1 & -1\end{pmatrix}, \quad \mp\begin{pmatrix}-1 & -2\\ 2 & -1\end{pmatrix},$$

$$\mp\begin{pmatrix}2 & -3\\ 1 & 1\end{pmatrix}, \quad \mp\begin{pmatrix}2 & -1\\ 1 & 2\end{pmatrix},$$

$$\mp\begin{pmatrix}-1 & -3\\ 1 & -2\end{pmatrix}, \quad \mp\begin{pmatrix}-2 & -1\\ 1 & -2\end{pmatrix};$$

$M_2(5)$ has 6 elements:

$$\mp\begin{pmatrix}1 & 3\\ -2 & -1\end{pmatrix}, \quad \mp\begin{pmatrix}1 & -2\\ 1 & 3\end{pmatrix}, \quad \mp\begin{pmatrix}-3 & -2\\ 1 & -1\end{pmatrix};$$

$M_3(5)$ has 4 elements:

$$\mp\begin{pmatrix}0 & -5\\ 1 & 3\end{pmatrix}, \quad \mp\begin{pmatrix}-3 & -5\\ 1 & 0\end{pmatrix}.$$

$M_1(7)$ has 90, $M_2(7)$ has 6, $M_3(7)$ has 10, $M_1(11)$ has 190 elements, etc.

5. The first existence theorem

In this and the following paragraphs we shall prove some theorems, which show that every element of $M(P)$ actually occurs in the set $\Omega(\zeta)$ of a certain P-adic number ζ; if the element lies in $M_2(P)$ or $M_3(P)$, then it may, however, be necessary to choose λ appropriately.

THEOREM 2: *Let*

$$\{\Omega_{n+1}\} = \{\Omega_1, \Omega_2, \Omega_3, \cdots\}, \quad \Omega_{n+1} = \begin{pmatrix} \alpha_{n+1}, & \alpha'_{n+1} \\ \beta_{n+1}, & \beta'_{n+1} \end{pmatrix},$$

be an infinite sequence of integer matrices of determinant P, and define a second sequence of matrices

$$\{\mathrm{T}_n\} = \{\mathrm{T}_0, \mathrm{T}_1, \mathrm{T}_2, \cdots\}$$

by

$$\mathrm{T}_0 = \mathrm{E}, \qquad \mathrm{T}_n = \Omega_1\Omega_2 \cdots \Omega_n = \begin{pmatrix} p_n & p'_n \\ q_n & q'_n \end{pmatrix} \quad \text{for} \quad n = 1, 2, 3, \cdots.$$

Then there is a P-adic integer ζ such that $\{\Omega_{n+1}\} = \Omega(\zeta)$ and $\{\mathrm{T}_n\} = \mathrm{T}(\zeta)$, if and only if $(q_n, q'_n) = 1$ and $\dfrac{-q'_n\lambda + p'_n}{q_n\lambda - p_n}$ lies in F for $n = 0, 1, 2, \cdots$.

PROOF: That the conditions are necessary, was already shown in §2; therefore we have only to prove that they are sufficient.

As in §2, let q_n^* be that one of the two numbers q_n and q'_n which is not divisible by P, and p_n^* the corresponding other element of T_n. Then there is exactly one integer A_n such that

$$p_n^* + q_n^* A_n \equiv 0 \pmod{P^n}, \qquad 0 \leqq A_n \leqq P^n - 1,$$

and since $P \nmid q_n^*$ and $p_n q'_n - p'_n q_n = P^n$, obviously

$$p_n + q_n A_n \equiv 0 \pmod{P^n}, \qquad p'_n + q'_n A_n \equiv 0 \pmod{P^n}.$$

Therefore there are two integers r_n and r'_n such that

$$p_n = P^n r_n - A_n q_n, \qquad p'_n = P^n r'_n - A_n q'_n,$$

and the determinant $r_n q'_n - r'_n q_n = 1$. Thus if

$$Z_n = \frac{A_n + \lambda}{P^n} \quad \text{and} \quad z_n = \frac{-q'_n Z_n + r'_n}{q_n Z_n - r_n},$$

then

$$z_n = \frac{-q'_n\lambda + p'_n}{q_n\lambda - p_n}$$

lies in F by hypothesis.

I assert that

$$A_{n+1} \equiv A_n \pmod{P^n}.$$

For

$$\mathrm{T}_{n+1} = \mathrm{T}_n \Omega_{n+1} = \begin{pmatrix} p_n \alpha_{n+1} + p'_n \beta_{n+1}, & p_n \alpha'_{n+1} + p'_n \beta'_{n+1} \\ q_n \alpha_{n+1} + q'_n \beta_{n+1}, & q_n \alpha'_{n+1} + q'_n \beta'_{n+1} \end{pmatrix},$$

hence

$$p_{n+1} + q_{n+1} A_n \equiv p_{n+1} + q_{n+1} A_{n+1} \equiv p'_{n+1} + q'_{n+1} A_n \equiv p'_{n+1} + q'_{n+1} A_{n+1} \equiv 0 \pmod{P^n},$$

from which the congruence follows immediately. If ζ is defined by

$$\zeta = \lim_{n \to \infty} A_n,$$

then this limit exists as a P-adic integer and satisfies all the conditions.

COROLLARY: *Let* $\mathrm{T} = \begin{pmatrix} p & p' \\ q & q' \end{pmatrix}$ *be an integer matrix of determinant* P^n, *such that* $(q, q') = 1$, *and* $\dfrac{-q'\lambda + p'}{q\lambda - p}$ *lies in* F. *Then there is a* P*-adic integer* ζ, *such that* T *is the element of* $\mathrm{T}(\zeta)$ *with index* n.

PROOF: We define the integer A_n by

$$p + A_n q \equiv p' + A_n q' \equiv 0 \pmod{P}, \qquad 0 \leqq A_n \leqq P^n - 1,$$

and take a P-adic integer ζ, for which $| \zeta - A_n |_P \leqq P^{-n}$; then by the proof of the last theorem, ζ satisfies all conditions.

6. The second existence theorem

THEOREM 3: *Let* z^* *be an arbitrary number in* F, α *and* β *two relatively prime integers,* ϵ *an arbitrarily small positive number. Then there is an index* $n > 0$ *and a* P*-adic integer* ζ, *such that the elements* $\mathrm{T}_n = \begin{pmatrix} p_n & p'_n \\ q_n & q'_n \end{pmatrix}$ *of* $\mathrm{T}(\zeta)$ *and* z_n *of* $z(\zeta)$ *satisfy the conditions*

$$\alpha q_n + \beta q'_n \equiv \mp 1 \pmod{P}, \qquad | z_n - z^* | \leqq \epsilon.$$

PROOF: Since $(\alpha, \beta) = 1$, there is an integer unimodular matrix

$$\Omega = \begin{pmatrix} \alpha & \alpha' \\ \beta & \beta' \end{pmatrix}.$$

Let D be the set of all points z in the upper half plane H, for which

$$\Omega z = \frac{\alpha z + \alpha'}{\beta z + \beta'}$$

satisfies the conditions

$$\Omega z \text{ lies in } F, \qquad | \Omega z - z^* | \leqq \epsilon.$$

Obviously this set has at least one inner point, say the point μ.

For $\eta = \mp 1$, consider the matrix $\Phi_\eta = \begin{pmatrix} 0 & -P \\ 1 & \eta \end{pmatrix}$ of determinant P, and the corresponding substitution

$$z' = \frac{-P}{z+\eta} = \Phi_\eta z.$$

Obviously, this can be written as

$$\frac{2z' + \eta - (1-4P)^{\frac{1}{2}}}{2z' + \eta + (1-4P)^{\frac{1}{2}}} = \vartheta \frac{2z + \eta - (1-4P)^{\frac{1}{2}}}{2z + \eta + (1-4P)^{\frac{1}{2}}},$$

where the factor

$$\vartheta = \frac{\eta - (1-4P)^{\frac{1}{2}}}{\eta + (1-4P)^{\frac{1}{2}}}$$

is a complex number of modulus 1. Since

$$\vartheta^2 + \left(2 - \frac{1}{P}\right)\vartheta + 1 = 0,$$

ϑ is not an algebraic integer, and therefore not a root of unity. Hence the powers $\vartheta^{-1}, \vartheta^{-2}, \vartheta^{-3}, \cdots$ lie everywhere dense on the unit circle in the complex plane.

Therefore, if Z is an arbitrary point in the upper half-plane H, and $K_\eta(Z)$ the circle

$$\left| \frac{2z + \eta - (1-4P)^{\frac{1}{2}}}{2z + \eta + (1-4P)^{\frac{1}{2}}} \right| = \left| \frac{2Z + \eta - (1-4P)^{\frac{1}{2}}}{2Z + \eta + (1-4P)^{\frac{1}{2}}} \right|$$

through this point, then with z also $\Phi_\eta z$ lies on $K_\eta(Z)$, and the points

$$z, \quad \Phi_\eta^{-1} z, \quad \Phi_\eta^{-2} z, \quad \Phi_\eta^{-3} z, \quad \cdots \qquad \left(\Phi_\eta^{-1} z = \frac{-\eta z - P}{z}\right)$$

obtained from z by repeated application of Φ_η^{-1} lie everywhere dense on this circle.

Now it is easy to see that we can connect λ with μ by means of a continuous curve C, which consists of arcs of the two circles $K_{-1}(\lambda)$ and $K_{-1}(\mu)$ and of circles $K_\eta(k + \frac{1}{2} + (1-4P)^{\frac{1}{2}})$, where $\eta = \mp 1$ and $k = 0, 1, 2, \cdots$; for any two circles $K_{-1}(k + \frac{1}{2} + (1-4P)^{\frac{1}{2}})$ and $K_{+1}(\kappa + \frac{1}{2} + (1-4P)^{\frac{1}{2}})$, where $k = 0, 1, 2, \cdots$ and $k - \frac{1}{2} \leqq \kappa \leqq k + 3/2$, intersect. Let $\lambda, \lambda_1, \lambda_2, \cdots, \lambda_t, \mu$ be the successive end points of the arcs composing C. Then by alternate applications of powers of Φ_{-1}^{-1} and Φ_{+1}^{-1}, we can transform λ successively into points arbitrarily near to $\lambda_1, \lambda_2, \cdots, \lambda_t$, and finally into a point z^{**} near to μ, which lies in D. In this way, we obtain an integer matrix

$$\mathrm{T}^* = \begin{pmatrix} p^* & p^{*\prime} \\ q^* & q^{*\prime} \end{pmatrix} = \Phi_{+1}^{h_1} \Phi_{-1}^{k_1} \Phi_{+1}^{h_2} \cdots \Phi_{-1}^{k_u},$$

where the exponents h, k are integers $\geqq 0$, such that

$$\lambda = \mathrm{T}^* z^{**}, \quad \text{or} \quad z^{**} = \mathrm{T}^{*-1}\lambda;$$

the determinant of T^* is a power of P, say P^n. Since

$$\Phi_\eta \equiv \begin{pmatrix} 0 & 0 \\ 1 & \eta \end{pmatrix} \pmod{P},$$

necessarily

$$\mathrm{T}^* \equiv \begin{pmatrix} 0 & 0 \\ \mp 1 & \mp 1 \end{pmatrix} \pmod{P}.$$

Now put

$$z_n = \Omega z^{**}, \qquad \mathrm{T}_n = \mathrm{T}^*\Omega^{-1} = \begin{pmatrix} p_n & p_n' \\ q_n & q_n' \end{pmatrix},$$

so that

$$\lambda = \mathrm{T}_n z_n \quad \text{and} \quad z_n = \mathrm{T}_n^{-1}\lambda,$$

and, by the definition of D,

$$z_n \text{ lies in } F, \quad \text{and} \quad |z_n - z^*| \leqq \epsilon.$$

We have

$$\mathrm{T}^* = \mathrm{T}_n\Omega = \begin{pmatrix} p_n & p_n' \\ q_n & q_n' \end{pmatrix}\begin{pmatrix} \alpha & \alpha' \\ \beta & \beta' \end{pmatrix} \equiv \begin{pmatrix} 0 & 0 \\ \mp 1 & \mp 1 \end{pmatrix} \pmod{P};$$

therefore

$$\alpha q_n + \beta q_n' \equiv \mp 1 \pmod{P},$$

and from $p_n q_n' - q_n p_n' = P^n$ in particular $(q_n, q_n') = 1$. Hence, by the corollary to Theorem 2, the theorem follows immediately.

7. An application of Theorem 3

To every element Ω of $M(P)$ belongs a certain set $S(\Omega)$ of points z in F, such that the transformed points $\Omega^{-1}z$ also lie in F; this set has inner points, or consists of an arc of a curve, or of a single point, according as Ω belongs to $M_1(P)$, or to $M_2(P)$, or to $M_3(P)$.

THEOREM 4: *Let Ω be an element of $M_1(P)$. Then there is a P-adic integer ζ, such that Ω is an element of the sequence $\Omega(\zeta)$. Provided that λ is chosen suitably, this is also true, if Ω belongs to $M_2(P)$ or $M_3(P)$.*

PROOF: Suppose that z^* is a point of $S(\Omega)$, in particular an inner point, if Ω belongs to $M_1(P)$. If $\Omega = \begin{pmatrix} \alpha & \alpha' \\ \beta & \beta' \end{pmatrix}$, then either $(\alpha, \beta) = 1$ or $(\alpha', \beta') = 1$, for $\alpha\beta' - \alpha'\beta = P$. Denote the pair, which is relatively prime, by α^*, β^*. Then,

by the last theorem, we can find a P-adic integer ζ_0 for which z_n is arbitrarily near to z^*, and for which $\mathrm{T}_n = \begin{pmatrix} p_n & p_n' \\ q_n & q_n' \end{pmatrix}$ satisfies the condition

$$\alpha^* q_n + \beta^* q_n' \equiv \mp 1 \not\equiv 0 \pmod{P}.$$

Thus, in particular, if

$$\mathrm{T}_{n+1} = \begin{pmatrix} p_{n+1} & p_{n+1}' \\ q_{n+1} & q_{n+1}' \end{pmatrix} = \mathrm{T}_n \Omega,$$

then $(q_{n+1}, q_{n+1}') = 1$, since one of the q's is not divisible by P.

Now, if Ω lies in $M_1(P)$, then we can choose ζ_0 in such a way that z_n lies in $S(\Omega)$. If, however, Ω is an element of $M_2(P)$ or $M_3(P)$, then by a slight change of λ, so that z_n remains in F, we can again obtain a ζ_0 for which z_n lies in $S(\Omega)$. Hence in both cases the number

$$z_{n+1} = \Omega^{-1} z_n = \mathrm{T}_{n+1}^{-1} \lambda$$

lies in F. Therefore by the corollary to Theorem 2 there is another P-adic integer ζ, such that Ω and z_{n+1} are the elements of $\Omega(\zeta)$ and $z(\zeta)$ with index $n+1$. The proof of Theorem 2 shows that necessarily $|\zeta - \zeta_0|_P \leqq P^{-n}$; hence T_n also belongs to $\mathrm{T}(\zeta)$, and Ω is an element of $\Omega(\zeta)$.

8. The sets $m(P)$ and $m'(P)$

Let $\Omega = \begin{pmatrix} \alpha & \alpha' \\ \beta & \beta' \end{pmatrix}$ be an element of $M(P)$. Then the fix points of the substitution

$$z' = \frac{\alpha z + \alpha'}{\beta z + \beta'} = \Omega z$$

satisfy the quadratic equation

$$\beta z^2 + (\beta' - \alpha) z - \alpha' = 0,$$

and are therefore

$$(15): \quad \frac{\alpha - \beta' \mp ((\alpha - \beta')^2 + 4\alpha'\beta)^{\frac{1}{2}}}{2\beta} = \frac{\alpha - \beta' \mp ((\alpha + \beta')^2 - 4P)^{\frac{1}{2}}}{2\beta},$$

if $\beta \neq 0$. Let us suppose that $\beta > 0$, and that both roots (15) are conjugate complex numbers, i.e., that $z' = \Omega z$ is an elliptic substitution. Then if

$$(16): \quad f_1 = \frac{\alpha - \beta' + ((\alpha + \beta')^2 - 4P)^{\frac{1}{2}}}{2\beta}, \qquad f_2 = \frac{\alpha - \beta' - ((\alpha + \beta')^2 - 4P)^{\frac{1}{2}}}{2\beta},$$

f_1 is the fix point with positive imaginary part, and f_2 the conjugate one. Obviously, $z' = \Omega z$ can be written as

$$(17): \quad \frac{z' - f_1}{z' - f_2} = \vartheta \frac{z - f_1}{z - f_2},$$

where the multiplicator

$$(18): \qquad \vartheta = \frac{\alpha - \beta f_1}{\alpha - \beta f_2} = \frac{\alpha + \beta' - ((\alpha + \beta')^2 - 4P)^{\frac{1}{2}}}{\alpha + \beta' + ((\alpha + \beta')^2 - 4P)^{\frac{1}{2}}}$$

satisfies the quadratic equation

$$(19): \qquad \vartheta^2 + \left(2 - \frac{(\alpha + \beta')^2}{P}\right)\vartheta + 1 = 0.$$

Let us now denote by $m'(P)$ and $m(P)$ the subset of those elements Ω of $M(P)$, which are elliptic, whose fix point f_1 lies in F, and whose multiplicator ϑ is a root of unity, or is not a root of unity, respectively.

For the elements Ω of $m'(P)$, the coefficient

$$2 - \frac{(\alpha + \beta')^2}{P}$$

in (19) obviously must be equal to 0, or to ∓ 1, or to ∓ 2. Hence necessarily $P = 2$ and $\alpha + \beta' = \mp 2$, or $P = 3$ and $\alpha + \beta' = \mp 3$, or P is arbitrary and $\alpha + \beta' = 0$. By the tables in §4, $m'(2)$ has six elements

$$\mp\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \qquad \mp\begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}, \qquad \mp\begin{pmatrix} 0 & 2 \\ -1 & 0 \end{pmatrix};$$

$m'(3)$ has six elements

$$\mp\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}, \qquad \mp\begin{pmatrix} -1 & 1 \\ -1 & -2 \end{pmatrix}, \qquad \mp\begin{pmatrix} 0 & 3 \\ -1 & 0 \end{pmatrix};$$

and $m'(5)$ has four elements

$$\mp\begin{pmatrix} 1 & 3 \\ -2 & -1 \end{pmatrix}, \qquad \mp\begin{pmatrix} 0 & 5 \\ -1 & 0 \end{pmatrix}.$$

If $P \geqq 5$ and Ω belongs to $m'(P)$, then $\alpha + \beta' = 0$, so that

$$\Omega = \begin{pmatrix} \alpha & \alpha' \\ \beta & -\alpha \end{pmatrix} \quad \text{and therefore} \quad \Omega^2 = -P\mathrm{E}.$$

Also in the case of $m'(2)$ and $m'(3)$

$$\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}^2 = 2\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}^2 = 2\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

and

$$\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}^2 = 3\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} -1 & 1 \\ -1 & -2 \end{pmatrix}^2 = 3\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

Hence no element Ω of $m'(P)$ can occur twice in succession in the sequence $\Omega(\zeta)$, since otherwise all elements T_n of $\mathrm{T}(\zeta)$ with sufficiently large n would no longer satisfy the condition $(q_n, q_n') = 1$.

For the elements of $m(P)$,

(20): $$\alpha + \beta' \not\equiv 0 \pmod{P}.$$

For Ω is elliptic, and therefore

$$(\alpha + \beta')^2 - 4P < 0, \quad \text{i.e.} \quad |\alpha + \beta'| < 2\sqrt{P},$$

and so, if (20) were not true,

$$P < 2\sqrt{P} \quad \text{or} \quad P < 4.$$

The tables in §4 show, however, that (20) holds also for $P = 2$ and $P = 3$.

9. A congruence for the powers of a matrix

Let $\Omega = \begin{pmatrix} \alpha & \alpha' \\ \beta & \beta' \end{pmatrix}$ be an element of $m(P)$, or more generally any elliptic integer matrix with determinant P^g ($g \geqq 1$), for which (20) is satisfied. Then the equation

(21): $$\begin{vmatrix} \alpha - \varphi & \alpha' \\ \beta & \beta' - \varphi \end{vmatrix} = \varphi^2 - (\alpha + \beta')\varphi + P^g = 0$$

has two different roots φ_1 and φ_2 in the field of the P-adic numbers. For define $((\alpha + \beta')^2 - 4P^g)^{\frac{1}{2}}$ as a P-adic integer by the convergent series

$$((\alpha + \beta')^2 - 4P^g)^{\frac{1}{2}} = (\alpha + \beta')\left\{1 - \frac{4P^g}{(\alpha + \beta')^2}\right\}^{\frac{1}{2}}$$

$$= (\alpha + \beta')\left\{1 - \frac{2P^g}{(\alpha + \beta')^2} - \frac{2^2P^{2g}}{(\alpha + \beta')^4 \cdot 2!} - \frac{1 \cdot 3 \cdot 2^3 P^{3g}}{(\alpha + \beta')^6 \cdot 3!} - \cdots\right\};$$

then these roots are given by

(22): $$\varphi_1 = \frac{\alpha + \beta' + ((\alpha + \beta')^2 - 4P^g)^{\frac{1}{2}}}{2}, \quad \varphi_2 = \frac{\alpha + \beta' - ((\alpha + \beta')^2 - 4P^g)^{\frac{1}{2}}}{2}.$$

Obviously

(23): $$\varphi_1 \equiv \alpha + \beta' \not\equiv 0 \pmod{P}, \qquad \varphi_2 \equiv 0 \pmod{P}.$$

It is well known that for every integer $k \geqq 0$

(24): $$\Omega^k = \varphi_1^k \frac{\Omega - \varphi_2 \mathrm{E}}{\varphi_1 - \varphi_2} + \varphi_2^k \frac{\Omega - \varphi_1 \mathrm{E}}{\varphi_2 - \varphi_1}.$$

Hence, from (23),

(25): $$\Omega^k \equiv (\alpha + \beta')^{k-1}\Omega \pmod{P} \qquad \text{for } k \geqq 1.$$

More generally, if $\mathrm{T} = \begin{pmatrix} p & p' \\ q & q' \end{pmatrix}$ is an integer matrix of determinant P^m, put

$$\mathrm{T}^* = \begin{pmatrix} p^* & p^{*\prime} \\ q^* & q^{*\prime} \end{pmatrix} = \mathrm{T}\Omega^k.$$

Then, from (25),

(26): $$T^* \equiv (\alpha + \beta')^{k-1} T\Omega \pmod{P} \qquad \text{for } k \geqq 1.$$

Therefore $(q^*, q^{*\prime}) = 1$, *if*

$(\alpha, \beta) = 1$ and $\alpha q + \beta q' \not\equiv 0 \pmod{P}$, or

$$(\alpha', \beta') = 1 \quad \text{and} \quad \alpha' q + \beta' q' \not\equiv 0 \pmod{P}.$$

From the definition of T^*,

$$(\varphi_1 - \varphi_2)p^* = \varphi_1^k\{p(\alpha - \varphi_2) + p'\beta\} - \varphi_2^k\{p(\alpha - \varphi_1) + p'\beta\},$$
$$(\varphi_1 - \varphi_2)q^* = \varphi_1^k\{q(\alpha - \varphi_2) + q'\beta\} - \varphi_2^k\{q(\alpha - \varphi_1) + q'\beta\},$$

and therefore

(27): $$p^* - \frac{p(\alpha - \varphi_2) + p'\beta}{q(\alpha - \varphi_2) + q'\beta} q^* = \frac{\beta}{q(\alpha - \varphi_2) + q'\beta} \varphi_2^k P^m.$$

This identity shows that $-p^*/q^*$ tends to a P-adic limit for $k \to \infty$, since $|\varphi_2|_P < 1$, and that this limit lies in the quadratic field given by (21).

10. The third existence theorem

In §1, we defined a generalized distance $\rho(z_1, z_2)$ between two points z_1 and z_2 in F. With this definition, the following theorem holds:

THEOREM 5: *Let* $\Omega = \begin{pmatrix} \alpha & \alpha' \\ \beta & \beta' \end{pmatrix}$ *be an element of* $m(P)$, f_1 *its fix point in* F. *Then to every* $\epsilon > 0$ *there is a* P*-adic integer* ζ *such that for all sufficiently large* n

$$\rho(z_n, f_1) \leqq \epsilon.$$

PROOF: Let $\delta > 0$ be a constant to be assigned later, and α^*, β^* the pair α, β or α', β', for which $(\alpha^*, \beta^*) = 1$. By Theorem 3, we can determine an index m and a P-adic integer ζ_0 for which $T_m = \begin{pmatrix} p_m & p_m' \\ q_m & q_m' \end{pmatrix}$ and z_m satisfy the conditions

$$\alpha^* q_m + \beta^* q_m' \not\equiv 0 \pmod{P}, \qquad |z_m - f_1| \leqq \delta.$$

Suppose that

$$T_m = \Omega_1 \Omega_2 \cdots \Omega_m,$$

where $\Omega_1, \Omega_2, \cdots, \Omega_m$ are the m first elements of $\Omega(\zeta_0)$.

Let us form the matrices

$$T_{m+k}^* = \begin{pmatrix} p_{m+k}^* & p_{m+k}^{*\prime} \\ q_{m+k}^* & q_{m+k}^{*\prime} \end{pmatrix} = T_m \Omega^k \qquad (k = 1, 2, 3, \cdots),$$

and the numbers

$$z_{m+k}^* = \Omega^{-k} z_m, \qquad (k = 1, 2, 3, \cdots),$$

which lie in H. From (17) in §8, obviously

$$\frac{z^*_{m+k} - f_1}{z^*_{m+k} - f_2} = \vartheta^{-k} \frac{z_m - f_1}{z_m - f_2},$$

where f_1 and f_2 are the fix points and ϑ the multiplicator of Ω. Since Ω belongs to $m(P)$, ϑ is a complex number of modulus 1, which is not a root of unity. Hence the points z^*_{m+k} for $k = 1, 2, 3, \cdots$ lie on a circle K given by

$$\left|\frac{z^* - f_1}{z^* - f_2}\right| = \left|\frac{z_m - f_1}{z_m - f_2}\right|,$$

and lie everywhere dense on K. To every point z^* on K, there is a point z, equivalent with respect to Γ, in F; it is obvious that we can choose δ and therefore also the radius of K so small that all these points satisfy the inequality

$$\rho(z, f_1) \leqq \epsilon.$$

Hence, in particular, if z_{m+k} is the point in F which is equivalent to z^*_{m+k}, then

$$\rho(z_{m+k}, f_1) \leqq \epsilon \qquad (k = 1, 2, 3, \cdots).$$

Now by the definition of equivalence,

$$z^*_{m+k} = \mathrm{P}_{m+k} z_{m+k} \qquad (k = 1, 2, 3, \cdots),$$

where P_{m+k} is an element of Γ. Similarly

$$z^*_{m+k+1} = \mathrm{P}_{m+k+1} z_{m+k+1}.$$

From

$$\Omega z^*_{m+k+1} = z^*_{m+k}$$

and from the two preceding equations,

(28): $$z_{m+k} = \Omega_{m+k+1} z_{m+k+1} \qquad (k = 1, 2, 3, \cdots),$$

where

$$\Omega_{m+k+1} = \mathrm{P}^{-1}_{m+k} \Omega \mathrm{P}_{m+k+1}.$$

If

$$\Omega_{m+1} = \Omega \mathrm{P}_{m+1},$$

then (28) holds also for $k = 0$.

Put

$$\mathrm{T}_n = \begin{pmatrix} p_n & p'_n \\ q_n & q'_n \end{pmatrix} = \mathrm{T}^*_n \mathrm{P}_n = \mathrm{T}_m \Omega^{n-m} \mathrm{P}_n \qquad (n > m),$$

so that

$$\mathrm{T}_n = \Omega_1 \Omega_2 \cdots \Omega_n, \qquad z_n = \mathrm{T}^{-1}_n \lambda \qquad \text{for } n \geqq m.$$

Then

$$(q_n, q'_n) = 1.$$

For if both q_n and q'_n were divisible by P, then the same would be true for q_n^* and $q_n^{*\prime}$ in

$$\mathrm{T}_n^* = \begin{pmatrix} p_n^* & p_n^{*\prime} \\ q_n^* & q_n^{*\prime} \end{pmatrix} = \mathrm{T}_n \mathrm{P}_n^{-1} = \mathrm{T}_m \Omega^{n-m}.$$

But by the last paragraph

$$\mathrm{T}_n^* \equiv (\alpha + \beta')^{n-m-1} \mathrm{T}_m \Omega \pmod{P} \qquad (n \geqq m+1),$$

and therefore by the construction of T_m, either q_n^* or $q_n^{*\prime}$ is not divisible by P.

It is now clear that the sequence of matrices

$$\mathrm{T}_0 = \mathrm{E}, \qquad \mathrm{T}_n = \Omega_1 \Omega_2 \cdots \Omega_n \qquad (n = 1, 2, 3, \cdots)$$

satisfies the conditions of Theorem 2. Hence there is a P-adic integer ζ (for which, by the way, obviously $|\zeta - \zeta_0|_P \leqq P^{-m}$), such that $\{\mathrm{T}_n\} = \mathrm{T}(\zeta)$ and $\{\Omega_n\} = \Omega(\zeta)$. By construction, the elements z_n of $z(\zeta)$ with $n \geqq m+1$ satisfy the required inequality $\rho(z_n, f_1) \leqq \epsilon$.

COROLLARY: *If ζ is the P-adic integer given by Theorem 5, then, for an infinity of indices,*

$$\mathrm{T}_n = \mathrm{T}_m \Omega^{n-m}, \qquad \Omega_n = \Omega.$$

In particular, these two equations are true for all sufficiently large n, if the fix point f_1 of Ω is an inner point of F.

PROOF: Let K be the circle defined in the proof of the preceding theorem. Since f_1 belongs to F, the points of K in F will form an arc of positive length; if, in particular, f_1 is an inner point of F, and ϵ, i.e. δ is sufficiently small, then K lies entirely in F. Hence in the former case an infinity of z_{m+k}^*, in the latter case all z_{m+k}^* with $k \geqq 0$, will lie in F, and the statements follow immediately from the proof of Theorem 5.

REMARK: Since $\mathrm{T}_n = \mathrm{T}_m \Omega^{n-m}$ for an infinity of indices n, formula (27) in §9 shows that ζ is a quadratic irrational P-adic number. Its sequence $\Omega(\zeta)$ will consist only of matrices Ω for large indices, if f_1 is an inner point of F and ϵ is sufficiently small; hence in this case $\Omega(\zeta)$ will be periodic. If, on the other hand, f_1 is not an inner point of F, or ϵ is not small enough, then the points z_{m+k}^* will not all belong to F, and since ϑ is not a root of unity, it is easy to see that $\Omega(\zeta)$ is not periodic for large indices. Hence Lagrange's Theorem on the periodicity of the continued fraction of a real quadratic irrational number has no analogue for P-adic numbers.

11. The function $Y(P)$

For every element Ω of $m(P)$, let $y(\Omega)$ be the imaginary part of the fix point f_1 of Ω in F, and put

(29): $$Y(P) = \min y(\Omega),$$

where the minimum refers to all elements of $m(P)$. Obviously

(30): $$Y(P) \geqq \frac{\sqrt{3}}{2}.$$

For $P \leqq 5$, the tables in §4 give

$$Y(2) = \frac{\sqrt{7}}{2}, \qquad Y(3) = \sqrt{2}, \qquad Y(5) = 1,$$

corresponding to the matrices

$$\begin{pmatrix} 1 & -2 \\ 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1 & -2 \\ 1 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}$$

with fix points

$$\frac{1 \mp \sqrt{-7}}{2}, \qquad \mp\sqrt{-2}, \qquad \mp i,$$

and multiplicators

$$\frac{-3 - \sqrt{-7}}{4}, \qquad \frac{-1 - 2\sqrt{-2}}{3}, \qquad \frac{3 - 4i}{5}.$$

THEOREM 6: $Y(P) = \frac{\sqrt{3}}{2}$, *if and only if* $P \equiv 1 \pmod 6$.

PROOF: We have to find all matrices $\Omega = \begin{pmatrix} \alpha & \alpha' \\ \beta & \beta' \end{pmatrix}$ of $m(P)$ with their fix point f_1 at $\rho = \frac{-1 + \sqrt{-3}}{2}$. This condition will be satisfied if

$$\beta\rho^2 + (\beta' - \alpha)\rho - \alpha' = 0,$$

or, since ρ is a root of the irreducible equation $\rho^2 + \rho + 1 = 0$, if

$$\alpha' = -\beta \quad \text{and} \quad \beta' = \alpha + \beta.$$

Therefore

$$\Omega = \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha + \beta \end{pmatrix} \quad \text{and} \quad \alpha^2 + \alpha\beta + \beta^2 = \tfrac{1}{4}\{(2\alpha + \beta)^2 + 3\beta^2\} = P.$$

Hence either $P = 3$ or $P \equiv 1 \pmod 6$. If $P = 3$, then necessarily

$$\Omega = \begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix} \quad \text{or} \quad \Omega = \begin{pmatrix} -1 & 1 \\ -1 & -2 \end{pmatrix},$$

and these matrices do not belong to $m(P)$. If, however, $P \equiv 1 \pmod 6$, then β is not divisible by P, so that

$$2 - \frac{(\alpha + \beta')^2}{P} = -2 + \frac{3\beta^2}{P}$$

is not an integer; hence the matrix $\Omega = \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha + \beta \end{pmatrix}$ now does belong to $m(P)$ and has ρ as its fix point f_1.

It is very probable that

$$\lim_{P\to\infty} Y(P) = \frac{\sqrt{3}}{2},$$

but so far I have not been able to prove this.[9a]

For $P \leqq 103$, $Y(P)$ is given in the following table:

P	$Y(P)$	P	$Y(P)$	P	$Y(P)$
2	$\sqrt{(7)/2}$	29	$\sqrt{(91)/10}$	67	$\sqrt{(3)/2}$
3	$\sqrt{(2)}$	31	$\sqrt{(3)/2}$	71	$5.\sqrt{(11)/18}$
5	1	37	$\sqrt{(3)/2}$	73	$\sqrt{(3)/2}$
7	$\sqrt{(3)/2}$	41	$\sqrt{(8)/3}$	79	$\sqrt{(3)/2}$
11	$\sqrt{(35)/6}$	43	$\sqrt{(3)/2}$	83	$\sqrt{(74)/9}$
13	$\sqrt{(3)/2}$	47	$\sqrt{(187)/14}$	89	$2.\sqrt{(10)/7}$
17	$\sqrt{(8)/3}$	53	$\sqrt{(91)/10}$	97	$\sqrt{(3)/2}$
19	$\sqrt{(3)/2}$	59	$\sqrt{(55)/8}$	101	$\sqrt{(65)/9}$
23	$\sqrt{(91)/10}$	61	$\sqrt{(3)/2}$	103	$\sqrt{(3)/2}$

12. The function $Y(\zeta)$

Let x_n and y_n be the real and imaginary parts of the n-th element $z_n = x_n + iy_n$ of the representative $z(\zeta)$ of a P-adic integer ζ. Suppose that

(31): $$Y(\zeta) = \limsup_{n\to\infty} y_n;$$

i.e. $Y(\zeta)$ is the greatest number, such that for every $\epsilon > 0$ and an infinity of indices

$$y_n \geqq Y(\zeta) - \epsilon.$$

Obviously

(32): $$Y(\zeta) \geqq \sqrt{(3)/2}.$$

THEOREM 7: *To every positive number ϵ, there is a P-adic integer ζ, for which*

$$Y(\zeta) \leqq Y(P) + \epsilon.$$

PROOF: Let Ω be an element of $m(P)$, such that $Y(P)$ is the imaginary part of its fix point f_1 in F. By Theorem 5, there is a P-adic integer ζ for any given $\delta > 0$, such that

$$\rho(z_n, f_1) = \min\left(|z_n - f_1|, |z_n - f_1 + 1|, |z_n - f_1 - 1|, \left|z_n + \frac{1}{f_1}\right|, \left|\frac{1}{z_n} + f_n\right|\right) \leqq \delta$$

for all sufficiently large n. This implies in particular

$$|y_n - Y(P)| \leqq \epsilon,$$

[9a] Addendum: This equation has now been proved by H. Davenport; see the following paper, these Annals, pp. 59–62.

if δ is chosen sufficiently small. For all points in the domain F':

$$|x| \leqq \tfrac{1}{2}, \qquad |z| \geqq 1,$$

which are equivalent to f_1, obviously have the same imaginary part $Y(P)$ as f_1; therefore the statement follows immediately from the continuity of the function $\rho(z, f_1)$.

Probably the following conjecture holds:

"*For every prime number P, and for every P-adic integer ζ,*

$$Y(\zeta) \geqq Y(P).$$"

For $P \equiv 1 \pmod 6$, thus in particular for $P = 7$, this conjecture is indeed true, as is evident from Theorem 6 and the trivial inequality (32). I shall prove the following three theorems, which show that it also holds for $P = 2$, $P = 3$, and $P = 5$, and therefore for all prime numbers less than 10.

13. The lower bound of $Y(\zeta)$ for $P = 2$, $P = 3$, and $P = 5$

THEOREM 8: *For every index n and for any diadic integer ζ*

$$\max(y_n, y_{n+1}, y_{n+2}) \geqq \frac{\sqrt{7}}{2}.$$

Hence in particular for all diadic integers ζ

$$Y(\zeta) \geqq \frac{\sqrt{7}}{2} = Y(2).$$

THEOREM 9: *For every index n and for any triadic integer ζ*

$$\max(y_n, y_{n+1}, y_{n+2}) \geqq \sqrt{2}.$$

Hence in particular for all triadic integers ζ

$$Y(\zeta) \geqq \sqrt{2} = Y(3).$$

THEOREM 10: *For every index n and for any pentadic integer ζ*

$$\max(y_n, y_{n+1}) \geqq 1.$$

Hence in particular for all pentadic integers ζ

$$Y(\zeta) \geqq 1 = Y(5).$$

The proofs of these three theorems depend on the following simple considerations. In

(33): $$z_n = \Omega_{n+1} z_{n+1},$$

Ω_{n+1} must be an element of $M(P)$, and both $z_n = x_n + iy_n$ and $z_{n+1} = x_{n+1} + iy_{n+1}$ must be points in F and therefore also in the closed domain F':

$$|x| \leqq \tfrac{1}{2}, \qquad |z| \geqq 1.$$

All we have to do is to determine, for every Ω in $M(P)$, the greatest partial domains S_n of points z_n and S_{n+1} of points z_{n+1} in F', which are related by (33) with $\Omega_{n+1} = \Omega$. In certain cases, these domains may degenerate into an arc of a circle or a segment of a straight line, or into a single point; if they contain inner points, then they are mapped conformally one upon the other.

For some of the elements of $M(P)$, one or the other of the domains S_n , S_{n+1} will contain only points, for which the ordinate $y_n(y_{n+1})$ is sufficiently large, e.g. $\geqq \sqrt{7}/2$ for $P = 2$. In other cases, both y_n and y_{n+1} may assume values smaller than the required bound, but not simultaneously, so that one of them always remains sufficiently large. In still other cases, both y_n and y_{n+1} will become too small at the same time. Then it is necessary to consider *two consecutive* (equal or different) elements Ω_{n+1} , Ω_{n+2} of $\Omega(\zeta)$, one of which is equal to Ω, and the three numbers z_n , z_{n+1} , $z_{n+2} = x_{n+2} + iy_{n+2}$ connected by

(34): $$z_n = \Omega_{n+1}z_{n+1} , \; z_{n+1} = \Omega_{n+2}z_{n+2} .$$

As in the simpler case above, there will be the three greatest domains S'_n , S'_{n+1} , S'_{n+2} of points z_n , z_{n+1} , z_{n+2} in F', which are connected by (34). The necessity for considering these sets of three domains will arise only in the proofs of Theorems 8 and 9. In all instances it will be easy to show that at least one of the numbers y_n , y_{n+1} , y_{n+2} is always sufficiently large. Only those combinations Ω_{n+1} , Ω_{n+2} have to be considered for which the simpler method fails; and when the product $\Omega_{n+1}\Omega_{n+2}$ is divisible by P, then also this combination can be excluded (compare §8).

Matrices Ω_{n+1} and $-\Omega_{n+1}$ lead to the same relations (33) or (34), so that only one of them has to be considered. Also our method is symmetrical in y_n and y_{n+1} in the case of a single matrix, and symmetrical in y_n and y_{n+2} in the case of two matrices. Hence in the first case, if one of the ordinates is sufficiently large for $\Omega_{n+1} = \Omega$, then the same will be true for $\Omega_{n+1} = \mp P\Omega^{-1}$; and in the second case, combinations Ω_{n+1} , Ω_{n+2} lead to the same bounds as $P\Omega_{n+2}^{-1}$, $P\Omega_{n+1}^{-1}$.

We arrange the steps of the proofs in the form of tables, so as to render them clearer.

14. **Proof of Theorem** 8

The elements

$$\mp\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \qquad \mp\begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}$$

of $M(2)$ satisfy the equations

$$\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}^2 = 2\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = 2\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$\begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}^2 = 2\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

Hence at least one of any two consecutive terms of $\Omega(\zeta)$ is different from these four matrices.

For the remaining elements of $M(2)$, the inequality

$$\max(y_n, y_{n+1}) \geqq \frac{\sqrt{7}}{2}$$

is satisfied, as follows from the following table:

Ω_{n+1}	S_n	S_{n+1}	Inequalities for y_n, y_{n+1}	$-P\Omega_{n+1}^{-1}$	Similar results for the matrices
$\begin{pmatrix} 0 & 2 \\ -1 & 0 \end{pmatrix}$			$\max(\lvert z_n\rvert, \lvert z_{n+1}\rvert) \geqq \sqrt{2}$, $\lvert x_n\rvert \leqq \frac{1}{2}$, $\lvert x_{n+1}\rvert \leqq \frac{1}{2}$, hence $\max(y_n, y_{n+1}) \geqq \frac{\sqrt{7}}{2}$		
$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$	$\lvert x_n\rvert \leqq \frac{1}{2}$, $\lvert z_n\rvert \geqq 2$	$\lvert z_{n+1}\rvert \leqq \frac{1}{4}$, $\lvert z_{n+1}\rvert \geqq 1$	$y_n \geqq \frac{\sqrt{15}}{2} > \frac{\sqrt{7}}{2}$	$\begin{pmatrix} -1 & 0 \\ 0 & -2 \end{pmatrix}$	
$\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$	$0 \leqq x_n \leqq \frac{1}{2}$, $\lvert z_n - 1\rvert \geqq 2$	$-\frac{1}{2} \leqq x_{n+1} \leqq -\frac{1}{4}$, $\lvert z_{n+1}\rvert \geqq 1$	$y_n \geqq \sqrt{3} > \frac{\sqrt{7}}{2}$	$\begin{pmatrix} -1 & 1 \\ 0 & -2 \end{pmatrix}$	$\begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} -1 & -1 \\ 0 & -2 \end{pmatrix}$
$\begin{pmatrix} 0 & -2 \\ -1 & 1 \end{pmatrix}$	$\lvert z_n - 2\rvert \leqq 2$, $\lvert z_n\rvert \geqq 1$, $x_n \leqq \frac{1}{2}$	$\lvert z_{n+1} - 1\rvert \leqq 2$, $\lvert z_{n+1} + 1\rvert \geqq 2$, $x_{n+1} \leqq \frac{1}{2}$	$y_{n+1} \geqq \frac{\sqrt{7}}{2}$	$\begin{pmatrix} -1 & 2 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 2 \\ -1 & -1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 \\ -1 & 0 \end{pmatrix}$

15. **Proof of Theorem** 9

We divide $M(3)$ into three subsets S_1, S_2, and S_3, where S_1 consists of the 6 elements

$$\mp\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}, \mp\begin{pmatrix} -1 & 1 \\ -1 & -2 \end{pmatrix}, \pm\begin{pmatrix} -1 & -2 \\ 2 & 1 \end{pmatrix},$$

S_2 of the 4 elements

$$\mp\begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}, \mp\begin{pmatrix} -1 & 2 \\ -1 & -1 \end{pmatrix},$$

and S_3 of the remaining 26 elements of $M(3)$. The relations

$$\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix} = 3\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} -1 & 1 \\ -1 & -2 \end{pmatrix} = 3\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$\begin{pmatrix} -1 & 1 \\ -1 & -2 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix} = 3\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \begin{pmatrix} -1 & 1 \\ -1 & -2 \end{pmatrix}\begin{pmatrix} -1 & 1 \\ -1 & -2 \end{pmatrix} = 3\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix},$$

$$\begin{pmatrix} -1 & -2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix} = 3\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \qquad \begin{pmatrix} -1 & -2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} -1 & 1 \\ -1 & -2 \end{pmatrix} = 3\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} -1 & -2 \\ 2 & 1 \end{pmatrix} = 3\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix},$$

$$\begin{pmatrix} -1 & 1 \\ -1 & -2 \end{pmatrix}\begin{pmatrix} -1 & -2 \\ 2 & 1 \end{pmatrix} = 3\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} -1 & -2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} -1 & -2 \\ 2 & 1 \end{pmatrix} = 3\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

show that at least one of any two consecutive terms of $\Omega(\zeta)$ does not belong to S_1.

Similarly it is evident from the equations

$$\begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix} = 3\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} -1 & 1 \\ -1 & -2 \end{pmatrix} = 3\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix},$$

$$\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} -1 & 2 \\ -1 & -1 \end{pmatrix} = 3\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}, \qquad \begin{pmatrix} -1 & 1 \\ -1 & -2 \end{pmatrix}\begin{pmatrix} -1 & 2 \\ -1 & -1 \end{pmatrix} = 3\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} -1 & -2 \\ 2 & 1 \end{pmatrix} = 3\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

$$\begin{pmatrix} -1 & -2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} -1 & 2 \\ -1 & -1 \end{pmatrix} = 3\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix},$$

that two consecutive terms of $\Omega(\zeta)$ cannot have the form

$$\Omega_{n+1} = \begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}, \qquad \Omega_{n+2} \text{ in } S_1 \quad \text{or} \quad \Omega_{n+1} \text{ in } S_1, \qquad \Omega_{n+2} = \begin{pmatrix} -1 & 2 \\ -1 & -1 \end{pmatrix}.$$

In the twelve remaining cases, we obtain the table shown on page 34.

Next, it is obvious from

$$\begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} -1 & 2 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ -1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix} = 3\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

that two consecutive elements of $\Omega(\zeta)$ cannot be

$$\Omega_{n+1} = \begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}, \qquad \Omega_{n+2} = \begin{pmatrix} -1 & 2 \\ -1 & -1 \end{pmatrix}$$

Ω_{n+1}	Ω_{n+2}	S'_n	S'_{n+1}	S'_{n+2}	Inequalities for y_n, y_{n+1}, y_{n+2}	Similar results for Ω_{n+1}	Similar results for Ω_{n+2}
$\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}$	$z_n = -\frac{1}{2} + \frac{9}{4t}i$, where $\frac{\sqrt{3}}{2} \leqq t \leqq \frac{3\sqrt{3}}{2}$	$z_{n+1} = \frac{9 - 4t^2 + 12it}{9 + 4t^2}$	$z_{n+2} = -\frac{1}{2} + it$	$\max(y_n, y_{n+2}) \geqq \frac{3}{2} > \sqrt{2}$	$\begin{pmatrix} -1 & 2 \\ -1 & -1 \end{pmatrix}$	$\begin{pmatrix} -1 & 1 \\ -1 & -2 \end{pmatrix}$
$\begin{pmatrix} -1 & 1 \\ -1 & -2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}$	$z_n = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$	$z_{n+1} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$	$z_{n+2} = -\frac{1}{2} + \frac{3\sqrt{3}}{2}i$	$y_{n+2} = \frac{3\sqrt{3}}{2} > \sqrt{2}$	$\begin{pmatrix} -1 & 2 \\ -1 & -1 \end{pmatrix}$	$\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}$
$\begin{pmatrix} -1 & -2 \\ 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}$	$z_n = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$	$z_{n+1} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$	$z_{n+2} = -\frac{1}{2} + \frac{3\sqrt{3}}{2}i$	$y_{n+2} = \frac{3\sqrt{3}}{2} > \sqrt{2}$	$\begin{pmatrix} -1 & 2 \\ -1 & -1 \end{pmatrix}$	$\begin{pmatrix} -1 & -2 \\ 2 & 1 \end{pmatrix}$

or

$$\Omega_{n+1} = \begin{pmatrix} -1 & 2 \\ -1 & -1 \end{pmatrix}, \qquad \Omega_{n+2} = \begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}.$$

It is, however, possible that $\Omega_{n+1} = \Omega_{n+2} = \begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}$, or

$$z_n = \frac{z_{n+1} + 2}{-z_{n+1} + 1} = \frac{-z_{n+2} + 4}{-2z_{n+2} - 1}, \qquad z_{n+1} = \frac{z_{n+2} + 2}{-z_{n+2} + 1}.$$

Then

$$y_n = \frac{9y_{n+2}}{(2x_{n+2} + 1)^2 + 2y_{n+2}^2}, \qquad y_{n+1} = \frac{3y_{n+2}}{(x_{n+2} - 1)^2 + 4y_{n+2}^2}.$$

Suppose that $y_{n+1} \leqq \sqrt{2}$, $y_{n+2} \leqq \sqrt{2}$, so that

$$\frac{3y_{n+2}}{(x_{n+2} - 1)^2 + y_{n+2}^2} \leqq \sqrt{2}, \qquad (x_{n+2} - 1)^2 \geqq y_{n+2}\left(\frac{3}{\sqrt{2}} - y_{n+2}\right).$$

Since $\sqrt{3}/2 \leqq y_{n+2} \leqq \sqrt{2}$, and $y\left(\frac{3}{\sqrt{2}} - y\right)$ assumes its minimum in any interval in one of its end points,

$$(x_{n+2} - 1)^2 \geqq \min\left(\sqrt{2}\left(\frac{3}{\sqrt{2}} - \sqrt{2}\right), \frac{\sqrt{3}}{2}\left(\frac{3}{\sqrt{2}} - \frac{\sqrt{3}}{2}\right)\right) = 1.$$

Therefore $-\frac{1}{2} \leqq x_{n+2} \leqq 0$, and finally

$$y_n \geqq \frac{9y_{n+2}}{1 + 4y_{n+2}^2} = \sqrt{2} + \frac{(4\sqrt{2}\, y_{n+2} - 1)(\sqrt{2} - y_{n+2})}{1 + 4y_{n+2}^2} \geqq \sqrt{2}.$$

A similar proof holds if

$$\Omega_{n+1} = \Omega_{n+2} = \begin{pmatrix} -1 & 2 \\ -1 & -1 \end{pmatrix}.$$

Our discussion has now exhausted all cases in which two consecutive elements of $\Omega(\zeta)$ belong to S_1 or S_2. There remain the elements of S_3; for these the table shown on page 36 is obtained.

16. **Proof of Theorem** 10

For $P = 5$, it is not necessary to consider *two consecutive* elements of $\Omega(\zeta)$, as we shall find that the theorem holds in its stronger form with only two ordinates.

$M(5)$ has 68 elements (see §4). Of these, only the following eight

$$\mp\begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}, \mp\begin{pmatrix} -2 & -1 \\ 1 & -2 \end{pmatrix}, \qquad \mp\begin{pmatrix} -1 & -2 \\ 2 & -1 \end{pmatrix}, \mp\begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix}$$

require particular examination.

Ω_{n+1}	S_n	S_{n+1}	Inequalities for y_n, y_{n+1}	$-P\Omega_{n+1}^{-1}$	Similar results for the matrices:—
$\begin{pmatrix} 0 & 3 \\ -1 & 0 \end{pmatrix}$			$\max(\lvert z_n\rvert, \lvert z_{n+1}\rvert) \geqq \sqrt{3}$, $\lvert x_n\rvert \leqq \frac{1}{2}$, $\lvert x_{n+1}\rvert \leqq \frac{1}{2}$, hence $\max(y_n, y_{n+1}) \geqq \frac{\sqrt{11}}{2} > \sqrt{2}$		
$\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}$	$\lvert x_n\rvert \leqq \frac{1}{2}$, $\lvert z_n\rvert \geqq 3$	$\lvert x_{n+1}\rvert \leqq \frac{1}{6}$, $\lvert z_{n+1}\rvert \geqq 1$	$y_n \geqq \frac{\sqrt{35}}{2} > \sqrt{2}$	$\begin{pmatrix} -1 & 0 \\ 0 & -3 \end{pmatrix}$	
$\begin{pmatrix} 3 & 1 \\ 0 & 1 \end{pmatrix}$	$\lvert x_n\rvert \leqq \frac{1}{2}$, $\lvert z_n - 1\rvert \geqq 3$	$-\frac{1}{2} \leqq x_{n+1} \leqq -\frac{1}{6}$, $\lvert z_{n+1}\rvert \geqq 1$	$y_n \geqq \frac{3\sqrt{3}}{2} > \sqrt{2}$	$\begin{pmatrix} -1 & 1 \\ 0 & -3 \end{pmatrix}$	$\begin{pmatrix} 3 & -1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} -1 & -1 \\ 0 & -3 \end{pmatrix}$
$\begin{pmatrix} 0 & 3 \\ -1 & 1 \end{pmatrix}$	$\lvert z_n\rvert \geqq 1$, $\lvert z_n - 3\rvert \leqq 3$, $x_n \leqq \frac{1}{2}$	$\lvert z_{n+1} + 2\rvert \geqq 3$, $\lvert z_{n+1} - 1\rvert \leqq 3$, $x_{n+1} \leqq \frac{1}{2}$	$y_{n+1} \geqq \frac{\sqrt{11}}{2} > \sqrt{2}$	$\begin{pmatrix} -1 & 3 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 3 \\ -1 & -1 \end{pmatrix}$, $\begin{pmatrix} 1 & 3 \\ -1 & 0 \end{pmatrix}$
$\begin{pmatrix} 0 & -3 \\ 1 & 2 \end{pmatrix}$	$z_n = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$	$z_{n+1} = -\frac{1}{2} + \frac{3\sqrt{3}}{2}i$	$y_{n+1} = \frac{3\sqrt{3}}{2} > \sqrt{2}$	$\begin{pmatrix} -2 & -3 \\ 1 & 0 \end{pmatrix}$	

If $\Omega_{n+1} = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}$, then

$$\lvert z_n\rvert^2 - 1 = 3\frac{\left(x_{n+1} - \frac{4}{3}\right)^2 + y_{n+1}^2 - \left(\frac{5}{3}\right)^2}{(x_{n+1} + 2)^2 + y_{n+1}^2},$$

$$y_n - 1 = -\frac{(x_{n+1}+2)^2 + \left(y_{n+1} - \frac{5}{2}\right)^2 - \left(\frac{5}{2}\right)^2}{(x_{n+1}+2)^2 + y_{n+1}^2}.$$

Now every point z_{n+1} for which

$$0 \leqq x_{n+1} \leqq \tfrac{1}{2}, \qquad |z_{n+1}| \geqq 1, \qquad y_{n+1} < 1,$$

lies inside the circle

$$(x_{n+1} - \tfrac{4}{3})^2 + y_{n+1}^2 = (\tfrac{5}{3})^2,$$

and every point for which

$$-\tfrac{1}{2} \leqq x_{n+1} \leqq 0, \qquad |z_{n+1}| \geqq 1, \qquad y_{n+1} < 1,$$

lies inside the second circle

$$(x_{n+1}+2)^2 + (y_{n+1} - \tfrac{5}{2})^2 = (\tfrac{5}{2})^2.$$

Hence in the first case $|z_n| < 1$, so that z_{n+1} does not belong to S_{n+1} ; in the second case $y_n > 1$. This proves that $\max(y_n, y_{n+1}) \geqq 1$ generally. The same result holds for $\begin{pmatrix} -2 & -1 \\ 1 & -2 \end{pmatrix} = -5\begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}^{-1}$.

Similarly, if $\Omega_{n+1} = \begin{pmatrix} -1 & -2 \\ 2 & -1 \end{pmatrix}$, then

$$|z_n|^2 - 1 = -3\frac{\left(x_{n+1} - \frac{4}{3}\right)^2 + y_{n+1}^2 - \left(\frac{5}{3}\right)^2}{(2x_{n+1}-1)^2 + 4y_{n+1}^2},$$

$$y_n - 1 = -4\frac{\left(x_{n+1} - \frac{1}{2}\right)^2 + \left(y_{n+1} - \frac{5}{8}\right)^2 - \left(\frac{5}{8}\right)^2}{(2x_{n+1}-1)^2 + 4y_{n+1}^2}.$$

Hence again the points z_{n+1} for which

$-\tfrac{1}{2} \leqq x_{n+1} \leqq 0$, $|z_{n+1}| \geqq 1$, $y_{n+1} < 1$, i.e. $(x_{n+1} - \tfrac{4}{3})^2 + y_{n+1}^2 - (\tfrac{5}{3})^2 > 0$,

do not belong to S_{n-1} , and $y_n > 1$ for all points z_{n+1} for which

$0 \leqq x_{n+1} \leqq \tfrac{1}{2}$, $|z_{n-1}| \geqq 1$, $y_{n+1} < 1$, i.e. $(x_{n+1} - \tfrac{1}{2})^2 + (y_{n+1} - \tfrac{5}{8})^2 - (\tfrac{5}{8})^2 < 0$.

Thus always $\max(y_n, y_{n+1}) \geqq 1$, and the same result holds for

$$\begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix} = -5\begin{pmatrix} -1 & -2 \\ 2 & -1 \end{pmatrix}^{-1}.$$

For the remaining 60 elements of $M(5)$, the table shown on page 38 is obtained:

Ω_{n+1}	S_n	S_{n+1}	Inequalities for y_n, y_{n+1}	$-5\Omega_{n+1}^{-1}$	Similar results for the matrices:—
$\begin{pmatrix} 0 & 5 \\ -1 & 0 \end{pmatrix}$			$\max(\lvert z_n\rvert, \lvert z_{n+1}\rvert) \geqq \sqrt{5}$, $\lvert x_n\rvert \leqq \frac{1}{2}, \lvert x_{n+1}\rvert \leqq \frac{1}{2}$, hence $\max(y_n, y_{n+1}) \geqq \frac{\sqrt{19}}{2} > 1.$		
$\begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}$	$\lvert x_n\rvert \leqq \frac{1}{2}, \lvert z_n\rvert \geqq 5$	$\lvert x_{n+1}\rvert \leqq \frac{1}{10}, \lvert z_{n+1}\rvert \geqq 1$	$y_n \geqq \frac{3\sqrt{11}}{2} > 1$	$\begin{pmatrix} -1 & 0 \\ 0 & -5 \end{pmatrix}$	
$\begin{pmatrix} 5 & 1 \\ 0 & 1 \end{pmatrix}$	$\lvert x_n\rvert \leqq \frac{1}{2}, \lvert z_n - 1\rvert \geqq 5$	$-\frac{3}{10} \leqq x_{n+1} \geqq \frac{1}{10}$, $\lvert z_{n+1}\rvert \geqq 1$	$y_n \geqq \frac{\sqrt{91}}{2} > 1$	$\begin{pmatrix} -1 & 1 \\ 0 & -5 \end{pmatrix}$	$\begin{pmatrix} 5 & -1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 0 & -5 \end{pmatrix}$
$\begin{pmatrix} 5 & 2 \\ 0 & 1 \end{pmatrix}$	$\lvert x_n\rvert \leqq \frac{1}{2}, \lvert z_n - 2\rvert \geqq 5$	$-\frac{1}{2} \leqq x_{n+1} \geqq -\frac{3}{10}$, $\lvert z_{n+1}\rvert \geqq 1$	$y_n \geqq \frac{5\sqrt{3}}{2} > 1$	$\begin{pmatrix} -1 & 2 \\ 0 & -5 \end{pmatrix}$	$\begin{pmatrix} 5 & -2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -2 \\ 0 & -5 \end{pmatrix}$
$\begin{pmatrix} 1 & -5 \\ 1 & 0 \end{pmatrix}$	$\lvert x_n\rvert \leqq \frac{1}{2}, \lvert z_n - 1\rvert \leqq 5$, $\lvert z_n + 4\rvert \geqq 5$	$x_{n+1} \leqq \frac{1}{2}, \lvert z_{n+1}\rvert \geqq 1$, $\lvert z_{n+1} - 5\rvert \leqq 5$, $\left\lvert z_{n+1} - \frac{5}{3}\right\rvert \geqq \frac{5}{3}$	$y_n \geqq \frac{\sqrt{19}}{2} > 1$	$\begin{pmatrix} 0 & -5 \\ 1 & -1 \end{pmatrix}$	$\begin{pmatrix} -1 & -5 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -5 \\ 1 & 1 \end{pmatrix}$

$\begin{pmatrix} 2 & -5 \\ 1 & 0 \end{pmatrix}$	$x_n \leqq \frac{1}{2}, \lvert z_n - 2 \rvert \leqq 5$ $\lvert z_n + 3 \rvert \geqq 5$	$x_{n+1} \leqq \frac{1}{2}, \lvert z_{n+1} \rvert \geqq 1$ $\left\lvert z_{n+1} - \frac{5}{2} \right\rvert \leqq \frac{5}{2}$	$y_n \geqq \frac{\sqrt{51}}{2} > 1$	$\begin{pmatrix} 0 & -5 \\ 1 & -2 \end{pmatrix}$	$\begin{pmatrix} -2 & -5 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -5 \\ 1 & 2 \end{pmatrix}$
$\begin{pmatrix} 1 & -4 \\ 1 & 1 \end{pmatrix}$	$\lvert x_n \rvert \leqq \frac{1}{2}, \lvert z_n + 4 \rvert \leqq 5$ $\left\lvert z_n + \frac{2}{3} \right\rvert \geqq \frac{5}{3}$	$\lvert x_{n+1} \rvert \leqq \frac{1}{2}, \lvert z_n - 4 \rvert \leqq 5$ $\left\lvert z_{n+1} - \frac{2}{3} \right\rvert \geqq \frac{5}{3}$	$\left.\begin{matrix} y_n \\ y_{n+1} \end{matrix}\right\} \geqq \frac{\sqrt{51}}{6} > 1$	$\begin{pmatrix} -1 & -4 \\ 1 & -1 \end{pmatrix}$	
$\begin{pmatrix} 2 & -3 \\ 1 & 1 \end{pmatrix}$	$\lvert x_n \rvert \leqq \frac{1}{2}, \lvert z_n + 3 \rvert \leqq 5$ $\left\lvert z_n - \frac{1}{3} \right\rvert \geqq \frac{5}{3}$	$\lvert x_{n+1} \rvert \leqq \frac{1}{2}, \lvert z_{n+1} \rvert \geqq 1$ $\left\lvert z_{n+1} - \frac{2}{3} \right\rvert \leqq \frac{5}{3}$	$y_n \geqq \frac{5\sqrt{3}}{6} > 1$	$\begin{pmatrix} -1 & -3 \\ 1 & -2 \end{pmatrix}$	$\begin{pmatrix} -2 & -3 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -3 \\ 1 & 2 \end{pmatrix}$
$\begin{pmatrix} 1 & 3 \\ -2 & -1 \end{pmatrix}$	$z_n = -\frac{1}{2} + ti,$ where $\frac{\sqrt{3}}{2} \leqq t \leqq \frac{5\sqrt{3}}{6}$	$z_{n+1} = -\frac{1}{2} + \frac{5}{4t} i$	$\max(y_n, y_{n+1})$ $\geqq \frac{\sqrt{5}}{2} > 1$		
$\begin{pmatrix} 1 & -2 \\ 1 & 3 \end{pmatrix}$	$z_n = \frac{-25 + 4t^2 + 20it}{25 + 4t^2}$ where $\frac{5\sqrt{3}}{6} \leqq t \leqq \frac{5\sqrt{3}}{2}$	$z_{n+1} = -\frac{1}{2} + ti$	$y_{n+1} \geqq \frac{5\sqrt{3}}{6} > 1$	$\begin{pmatrix} -3 & -2 \\ 1 & -1 \end{pmatrix}$	
$\begin{pmatrix} 0 & -5 \\ 1 & 3 \end{pmatrix}$	$z_n = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$	$z_{n+1} = -\frac{1}{2} + \frac{5\sqrt{3}}{2} i$	$y_{n+1} = \frac{5\sqrt{3}}{2} > 1$	$\begin{pmatrix} -3 & 5 \\ 1 & 0 \end{pmatrix}$	

17. A characteristic property of a rational number

Let us return to the case of a general prime number P, and divide the elements $\Omega = \begin{pmatrix} \alpha & \alpha' \\ \beta & \beta' \end{pmatrix}$ of $M(P)$ into two sets $M'(P)$ and $M''(P)$, such that

$$\beta \neq 0 \text{ for the elements of } M'(P),$$

and

$$\beta = 0 \text{ for the elements of } M''(P).$$

THEOREM 11. *Suppose that ζ is a P-adic integer. A necessary and sufficient condition that all elements of $\Omega(\zeta)$ with sufficiently large index belong to $M''(P)$, is that ζ is a rational number.*

PROOF: A) The condition is sufficient. Suppose that Ω_n belongs to $M''(P)$, say for all indices $n \geqq m+1$. Put

$$\Omega_{m,n} = \Omega_{m+1}\Omega_{m+2} \cdots \Omega_n,$$

so that

$$\mathbf{T}_n = \mathbf{T}_m \Omega_{m,n}.$$

Obviously

$$\Omega_{m,n} = \begin{pmatrix} P^a & Q \\ 0 & P^b \end{pmatrix},$$

where $a \geqq 0$, $b \geqq 0$ and Q are rational integers, and where $a + b = n - m$. Since both z_m and z_n lie in F, and

$$z_n = P^{b-a} z_m - P^{-a} Q,$$

necessarily

(35): $$\lim_{n \to \infty} b = +\infty.$$

But

$$\begin{pmatrix} p_n & p_n' \\ q_n & q_n' \end{pmatrix} = \begin{pmatrix} p_m & p_m' \\ q_m & q_m' \end{pmatrix} \begin{pmatrix} P^a & Q \\ 0 & P^b \end{pmatrix} = \begin{pmatrix} P^a p_m & Qp_m + P^b p_m' \\ P^a q_m & Qq_m + P^b q_m' \end{pmatrix},$$

and therefore by §2

$$P^a(p_m + q_m\zeta) \equiv 0 \pmod{P^n}, \quad \text{i.e.} \quad p_m + q_m\zeta \equiv 0 \pmod{P^{m+b}}.$$

Hence, from (35),

$$\zeta = P\text{-adic} \lim_{n \to \infty} \left(-\frac{p_m}{q_m} \right) = -\frac{p_m}{q_m},$$

as was to be proved.

B) The condition is necessary. Suppose that $\zeta = -p/q$, where $q \geqq 1$, and $(p, q) = 1$. Since ζ is a P-adic integer, $(P, q) = 1$.

To every index n, there is an integer A_n, such that

$$0 \leqq A_n \leqq P^n - 1, \qquad p + qA_n \equiv 0 \pmod{P^n},$$

and a second integer r_n, for which

$$p + qA_n = r_n P^n.$$

Hence

(36): $$(q, r_n) = 1,$$

since every common divisor of q and r_n is a divisor of p.

From (36), the equation

(37): $$r_n q_n' - r_n' q = 1$$

has integer solutions; if $q_n' = q_n^*$, $r_n' = r_n^*$ is one of them, then the general solution is given by

$$q_n' = q_n^* + kq, \qquad r_n' = r_n^* + kr_n,$$

where k is an arbitrary integer. We assume that this integer k is chosen such that the real part of the complex number

(38): $$z_n = -\frac{q_n'}{q} + \frac{P^n}{q(p - q\lambda)}$$

satisfies the inequalities

$$-\tfrac{1}{2} \leqq \Re(z_n) < \tfrac{1}{2}.$$

Obviously the imaginary part of the complex number $\dfrac{1}{q(p - q\lambda)}$ is positive.

Hence, if n is sufficiently large, z_n is a point in F.

Now, if as in §1,

$$Z_n = \frac{A_n + \lambda}{P^n} = \frac{-(p - q\lambda) + r_n P^n}{qP^n},$$

then it is easily verified that

(39): $$Z_n = \frac{r_n z_n + r_n'}{qz_n + q_n'}.$$

Hence z_n is the z_n of §1 for all sufficiently large n.

From (38), for two consecutive indices n and $n + 1$,

(40): $$z_n = \frac{z_{n+1} + \alpha_{n+1}'}{P}, \quad \text{where} \quad \alpha_{n+1}' = \frac{q_{n+1}' - Pq_n'}{q}.$$

Now $A_{n+1} = A_n + a_n P^n$ with an integer a_n, hence

$$p + qA_n = r_n P^n \quad \text{and} \quad p + q(A_n + a_n P^n) = r_{n+1} P^{n+1},$$

and therefore

$$r_n = Pr_{n+1} - qa_n.$$

Substituting this for r_n in (37) and subtracting the same equation with $n+1$ in place of n,

$$r_{n+1}(Pq'_n - q'_{n+1}) + q(r'_{n+1} - q'a_n - r'_n) = 0,$$

and finally from $(r_{n+1}, q) = 1$,

$$Pq'_n - q'_{n+1} \equiv 0 \pmod{q}.$$

Hence α'_{n+1} in (40) is an integer, and the matrix

$$\Omega_{n+1} = \begin{pmatrix} 1 & \alpha'_{n+1} \\ 0 & P \end{pmatrix}$$

of the transformation (40) is indeed an element of $M''(P)$, as was to be proved.

COROLLARY: *For a rational P-adic integer* ζ,

(41): $$\lim_{n\to\infty} y_n = +\infty.$$

PROOF: Immediate from (38).

18. A characteristic property of an irrational number

As we shall now prove, formula (41) is not true for irrational P-adic numbers. Put

(42): $$y(\zeta) = \liminf_{n\to\infty} y_n,$$

so that

$$\frac{\sqrt{3}}{2} \leqq y(\zeta) \leqq Y(\zeta).$$

THEOREM 12: *If* ζ *is an irrational P-adic integer, then for an infinity of indices* n

$$y_n \leqq \sqrt{P},$$

and therefore

(43): $$y(\zeta) \leqq \sqrt{P}.$$

PROOF: By Theorem 11, there are arbitrarily large indices $n+1$, for which $\Omega_{n+1} = \begin{pmatrix} \alpha_{n+1} & \alpha'_{n+1} \\ \beta_{n+1} & \beta'_{n+1} \end{pmatrix}$ does not belong to $M''(P)$, so that $\beta_{n+1} \neq 0$. Hence

$$z_n = \frac{\alpha_{n+1} z_{n+1} + \alpha'_{n+1}}{\beta_{n+1} z_{n+1} + \beta'_{n+1}}$$

can be written as

$$(\beta_{n+1} z_n - \alpha_{n+1})(\beta_{n+1} z_{n+1} + \beta'_{n+1}) = -P.$$

Therefore

$$\min\left(\left|z_n - \frac{\alpha_{n+1}}{\beta_{n+1}}\right|, \left|z_{n+1} + \frac{\beta'_{n+1}}{\beta_{n+1}}\right|\right) \leqq \frac{\sqrt{P}}{|\beta_{n+1}|},$$

or

$$\min(y_n, y_{n+1}) \leqq \frac{\sqrt{P}}{|\beta_{n+1}|},$$

and the statement follows immediately, since $|\beta_{n+1}| \geqq 1$.

The question arises, whether the constant $\sqrt{P}$ in Theorem 12 is the best possible. This question is answered in the affirmative by the following

THEOREM 13: *To every $\epsilon > 0$, there is an irrational P-adic integer ζ, for which*

$$y(\zeta) \geqq \sqrt{P} - \epsilon.$$

PROOF: Let g be a large positive integer, and Ω the elliptic matrix

$$\Omega = \begin{pmatrix} 0 & P^{g+1} \\ -P^g & -1 \end{pmatrix}$$

of determinant P^{2g+1}; we suppose that g is so large that the fix point

$$f_1 = \frac{-1 + (1 - 4P^{2g+1})^{\frac{1}{2}}}{2P^g}$$

of Ω in F satisfies the inequality

$$|f_1 - \sqrt{-P}| \leqq \delta,$$

where δ is a positive constant to be assigned later.

By Theorem 3, there is a P-adic integer ζ_0 and a positive integer m, such that if $\mathrm{T}_m = \begin{pmatrix} p_m & p'_m \\ q_m & q'_m \end{pmatrix}$ and z_m are the elements of $\mathrm{T}(\zeta)$ and $z(\zeta)$ of index m, then

(44): $$q'_m \not\equiv 0 \pmod{P}, \qquad |z_m - f_1| \leqq \delta.$$

Put

$$\Omega^*_{m+k(2g+1)+h} = \left\{ \begin{array}{ll} \begin{pmatrix} 0 & P \\ -1 & 0 \end{pmatrix} & \text{for } h = 1 \\ \begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix} & \text{for } h = 2, 3, \cdots, g \\ \begin{pmatrix} 1 & 1 \\ 0 & P \end{pmatrix} & \text{for } h = g+1 \\ \begin{pmatrix} P & 0 \\ 0 & 1 \end{pmatrix} & \text{for } h = g+2, g+3, \cdots, 2g+1 \end{array} \right\} \text{and } k = 0, 1, 2, \cdots,$$

and for $n \geqq m+1$

$$\mathrm{T}^*_n = \begin{pmatrix} p^*_n & p^{*\prime}_n \\ q^*_n & q^{*\prime}_n \end{pmatrix} = \mathrm{T}_m \Omega^*_{m+1} \Omega^*_{m+2} \cdots \Omega^*_n.$$

Since

$$\Omega^*_{m+k(2g+1)+1}\Omega^*_{m+k(2g+1)+2}\cdots\Omega^*_{m+(k+1)(2g+1)} = \begin{pmatrix} 0 & P \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix}^{g-1}\begin{pmatrix} 1 & 1 \\ 0 & P \end{pmatrix}\begin{pmatrix} P & 0 \\ 0 & 1 \end{pmatrix}^{g} = \Omega,$$

obviously

$$\mathrm{T}^*_{m+k(2g+1)+h} = \mathrm{T}_m\Omega^k\Omega^*_{m+k(2g+1)+1}\cdots\Omega^*_{m+k(2g+1)+h},$$

and in particular

$$\mathrm{T}^*_{m+k(2g+1)} = \mathrm{T}_m\Omega^k.$$

Hence, by formula (26) in §9,

$$\mathrm{T}^*_{m+k(2g+1)} \equiv (-1)^{k-1}\mathrm{T}_m\Omega \equiv (-1)^k\begin{pmatrix} 0 & p'_m \\ 0 & q'_m \end{pmatrix} \pmod{P}.$$

From the first condition (44), therefore, $(q^*_n, q^{*\prime}_n) = 1$ for $n = m + k(2g + 1)$, and this must remain true also for all other indices $n \geqq m + 1$, since T^*_n is a left-hand divisor of all $\mathrm{T}^*_{m+k(2g+1)}$ with greater index.

Let z^*_n be the complex number

$$z^*_n = (\Omega^*_{m+1}\Omega^*_{m+2}\cdots\Omega^*_n)^{-1}z_m = \mathrm{T}^{*-1}_n\lambda \qquad (n \geqq m + 1),$$

so that in particular

$$z^*_{m+k(2g+1)} = \Omega^{-k}z_m \qquad \text{and} \qquad z^*_{m+k(2g+1)+1} = \frac{-P}{z^*_{m+k(2g+1)}}.$$

As in §10, since Ω has the fix point f_1,

$$|z^*_{m+k(2g+1)} - f_1| \leqq \delta_1 \qquad \text{for } k = 0, 1, 2, \cdots,$$

and therefore

$$\left|z^*_{m+k(2g+1)+1} + \frac{P}{f_1}\right| \leqq \delta_2 \qquad \text{for } k = 0, 1, 2, \cdots,$$

where both $\delta_1 > 0$ and $\delta_2 > 0$ only depend on δ and tend to zero with δ. In the second inequality

$$-\frac{P}{f_1} = \frac{1 + (1 - 4P^{2g+1})^{\frac{1}{2}}}{2P^g}.$$

Suppose now that $\epsilon \leqq \frac{1}{3}$, and that δ is so small that

$$\max(\delta + \delta_1, \delta + \delta_2) \leqq \epsilon.$$

Then, from the definition of g and from the last formulae,

$$|z^*_{m+k(2g+1)+h} - \sqrt{-P}| \leqq \epsilon \qquad \text{for } h = 0 \text{ or } 1,\ k = 0, 1, 2, \cdots,$$

so that in particular all points

$$z^*_{m+k(2g+1)}, \qquad z^*_{m+k(2g+1)+1}$$

lie in F, and their imaginary parts satisfy

(45): $\quad \Im(z^*_{m+k(2g+1)+h}) \geqq \sqrt{P} - \epsilon \qquad$ for $h = 0$ or 1, $k = 0, 1, 2, \cdots$.

The remaining z^*_n are given by

$$z^*_{m+k(2g+1)+h} = \left.\begin{cases} P^{h-1} z^*_{m+k(2g+1)+1} & \text{for } h = 2, 3, \cdots, g \\ P^g z^*_{m+k(2h+1)+1} - 1 & \text{for } h = g+1 \\ P^{2g-h+1} z^*_{m+k(2g+1)+1} - P^{g-h-1} & \\ & \text{for } h = g+2, g+3, \cdots, 2g \end{cases}\right\} \text{and } k = 0, 1, 2, \cdots,$$

so that for these numbers

(46): $\quad \Im(z^*_{m+k(2g+1)+h}) \geqq P(\sqrt{P} - \epsilon) \qquad$ for $h = 2, 3, \cdots, 2g$, $k = 0, 1, 2, \cdots$.

Suppose now that for $n \geqq m + 1$, z_n is the point in F equivalent to z^*_n with respect to Γ, and that

$$z^*_n = \mathrm{P}_n z_n ,$$

where P_n belongs to Γ. Evidently

$$z_{m+k(2g+1)+h} = z^*_{m+k(2g+1)+h} , \qquad \mathrm{P}_{m+k(2g+1)+h} = \mathrm{E} \quad \text{for } h = 0 \text{ or } 1, k = 0, 1, 2, \cdots ,$$

and

(47): $$\Im(z_n) = \Im(z^*_n) \qquad \text{for } n \geqq m + 1.$$

Put

$$\Omega_{m+1} = \Omega^*_{m+1} \mathrm{P}_{m+1} = \Omega^*_{m+1} , \qquad \Omega_n = \mathrm{P}^{-1}_{n-1} \Omega^*_n \mathrm{P}_n \qquad \text{for } n \geqq m + 2,$$

and

$$\mathrm{T}_n = \begin{pmatrix} p_n & p'_n \\ q_n & q'_n \end{pmatrix} = \mathrm{T}_m \Omega_{m+1} \Omega_{m+2} \cdots \Omega_n \qquad \text{for } n \geqq m + 1,$$

so that

$$\mathrm{T}_n = \mathrm{T}^*_n \mathrm{P}_n ,$$

and therefore in particular

$$\mathrm{T}_{m+k(2g+1)+h} = \mathrm{T}^*_{m+k(2g+1)+h} \qquad \text{for } h = 0 \text{ or } 1, k = 0, 1, 2, \cdots .$$

Since $(q^*_n , q^{*\prime}_n) = 1$ and T_n is a left-hand divisor of $\mathrm{T}^*_n = \mathrm{T}_n \mathrm{P}^{-1}_n$, obviously also

$$(q_n , q'_n) = 1 \qquad (n \geqq m + 1).$$

Furthermore, all numbers

$$z_n = \mathrm{T}^{-1}_n \lambda$$

lie in F, as follows from the construction of z_n and T_n.

Hence, if

$$\{\Omega_1, \Omega_2, \cdots, \Omega_m\}, \qquad \{T_0, T_1, \cdots, T_m\}, \qquad \{z_0, z_1, \cdots, z_m\}$$

are the elements of $\Omega(\zeta_0)$, $T(\zeta_0)$, and $z(\zeta_0)$ with indices $n \leqq m$, we can apply Theorem 2 to the infinite sequences

$$\{\Omega_1, \Omega_2, \Omega_3, \cdots\}, \qquad \{T_0, T_1, T_2, \cdots\}, \qquad \{z_0, z_1, z_2, \cdots\}.$$

We obtain the existence of a P-adic integer ζ (for which, by the way, $|\zeta - \zeta_0|_P \leqq P^{-m}$), such that $\{\Omega_n\} = \Omega(\zeta)$, $\{T_n\} = T(\zeta)$, $\{z_n\} = z(\zeta)$. This number is irrational by Theorem 12, since

$$\Omega_{m+k(2g+1)+1} = \Omega^*_{m+k(2g+1)+1} = \begin{pmatrix} 0 & P \\ -1 & 0 \end{pmatrix} \qquad (k = 0, 1, 2, \cdots)$$

does not belong to $M''(P)$. (Formula (27) in §9 shows that ζ lies in a quadratic field; compare the proof of the next theorem.) Also from (45), (46), and (47),

$$y_n \geqq \sqrt{P} - \epsilon,$$

for all $n \geqq m$, so that ζ satisfies all conditions of Theorem 13.

19. Additions to the last theorems

THEOREM 14: *If ζ is the P-adic integer of Theorem* 13, *then*

$$\sqrt{P} - \epsilon \leqq y_n \leqq \sqrt{P}, \qquad |p_n + q_n\zeta|_P = P^{-n}$$

for an infinity of indices.

PROOF: We specialize the formulae in §9 by taking

$$\Omega = \begin{pmatrix} 0 & P^{g+1} \\ -P^g & -1 \end{pmatrix}, \qquad T = T_m = \begin{pmatrix} p_m & p'_m \\ q_m & q'_m \end{pmatrix},$$

$$T^* = T_{m+k(2g+1)} = \begin{pmatrix} p_{m+k(2g+1)} & p'_{m+k(2g+1)} \\ q_{m+k(2g+1)} & q'_{m+k(2g+1)} \end{pmatrix},$$

where these matrices are the same as those defined in the proof of the last theorem. The equation for φ_1 and φ_2 becomes

$$\varphi^2 + \varphi + P^{2g+1} = 0,$$

and its two roots satisfy

$$|\varphi_1|_P = 1, \qquad |\varphi_2|_P = P^{-(2g+1)}.$$

By (27),

$$p_{m+k(2g+1)} - \frac{p_m P^{-g}\varphi_2 + p'_m}{q_m P^{-g}\varphi_2 + q'_m} q_{m+k(2g+1)} = \frac{\varphi_2^k P^m}{q_m P^{-g}\varphi_2 + q'_m}.$$

Here $|P^{-g}\varphi_2|_P \leqq 1/P$, and $|q'_m|_P = 1$ by construction; hence

$$\zeta = -\frac{p_m P^{-g}\varphi_2 + p'_m}{q_m P^{-g}\varphi_2 + q'_m}$$

is a P-adic integer, for which

$$(48): \quad |\, p_{m+k(2g+1)} + q_{m+k(2g+1)}\,\zeta\,|_P = \left| \frac{\varphi_2^k P^m}{q_m P^{-g}\varphi_2 + q'_m} \right|_P = P^{-\{m+k(2g+1)\}};$$

i.e. ζ is the number of Theorem 13.

All points $z_{m+k(2g+1)}$ lie on a circle K, whose points z satisfy the inequalities

$$|\, z - \sqrt{-P}\,| \leqq \epsilon;$$

since f_1 is an inner point of K and since $\Im(f_1) < \sqrt{P}$, K must have an arc C, for whose points $\Im(z) \leqq \sqrt{P}$. Now the multiplicator ϑ of Ω is not a root of unity, if, as we assume, g is sufficiently large. Hence there are arbitrarily large integer values of k, for which $z_{m+k(2g+1)}$ lies on C, so that the theorem follows immediately.

The number ζ of the last two theorems had the property that all elements of $\Omega(\zeta)$ with sufficiently large indices were either equal to $\mp\begin{pmatrix} 0 & P \\ -1 & 0 \end{pmatrix}$ or belonged to $M''(P)$. This is not accidental, as the following theorem shows:

THEOREM 15: *If an infinity of elements of $\Omega(\zeta)$ belong to $M'(P)$, but are different from $\mp\begin{pmatrix} 0 & P \\ -1 & 0 \end{pmatrix}$, then*

$$y(\zeta) \leqq \frac{(4P-1)^{\frac{1}{2}}}{2} < \sqrt{P}.$$

To every $\epsilon > 0$, there is a number ζ with this property, for which

$$\frac{(4P-1)^{\frac{1}{2}}}{2} - \epsilon \leqq y(\zeta) \leqq \frac{(4P-1)^{\frac{1}{2}}}{2}.$$

PROOF: Let $\Omega_{n+1} = \begin{pmatrix} \alpha_{n+1} & \alpha'_{n+1} \\ \beta_{n+1} & \beta'_{n+1} \end{pmatrix} \neq \mp\begin{pmatrix} 0 & P \\ -1 & 0 \end{pmatrix}$ belong to $M'(P)$, so that $\beta_{n+1} \neq 0$ and

$$(\beta_{n+1}z_n - \alpha_{n+1})(\beta_{n+1}z_{n+1} + \beta'_{n+1}) = -P.$$

If $|\, \beta_{n+1}\,| \geqq 2$, then, as in §18,

$$\min(y_n, y_{n+1}) \leqq \frac{\sqrt{P}}{|\beta_{n+1}|} < \frac{(4P-1)^{\frac{1}{2}}}{2}.$$

If $|\, \beta_{n+1}\,| = 1$, $\alpha_{n+1}\beta'_{n+1} \neq 0$, then $|\, \beta_{n+1}x_n - \alpha_{n+1}\,| \geqq \frac{1}{2}$, $|\, \beta_{n+1}x_{n+1} - \beta'_{n+1}\,| \geqq \frac{1}{2}$; since $\min(|\, z_n\,|, |\, z_{n+1}\,|) \leqq \sqrt{P}$,

$$\min(y_n, y_{n+1}) \leqq ((\sqrt{P})^2 - (\tfrac{1}{2})^2)^{\frac{1}{2}} = \frac{(4P-1)^{\frac{1}{2}}}{2}.$$

Finally, if $|\, \beta_{n+1}\,| = 1$ and $\alpha_{n+1}\beta'_{n+1} = 0$, then Ω_{n+1} is one of the matrices

$$\mp\begin{pmatrix} 0 & 1 \\ -P & a \end{pmatrix}, \quad \mp\begin{pmatrix} -a & 1 \\ -P & 0 \end{pmatrix}, \quad \mp\begin{pmatrix} 0 & P \\ -1 & a \end{pmatrix}, \quad \mp\begin{pmatrix} -a & P \\ -1 & 0 \end{pmatrix},$$

where a is an integer. Of these matrices, $\mp\begin{pmatrix} 0 & 1 \\ -P & a \end{pmatrix}$ and $\mp\begin{pmatrix} -a & 1 \\ -P & 0 \end{pmatrix}$ do not belong to $M(P)$. If $\Omega_{n+1} = \mp\begin{pmatrix} 0 & P \\ -1 & a \end{pmatrix}$, then $a \neq 0$ and $z_n = -P/(z_{n+1} - a)$; hence

$$y_n = \frac{Py_{n+1}}{(x_{n+1} - a)^2 + y_{n+1}^2} \leqq \frac{4Py_{n+1}}{1 + 4y_{n+1}^2}$$

since $| x_{n+1} - a | \geqq \frac{1}{2}$, and therefore

$$y_n - \frac{(4P-1)^{\frac{1}{2}}}{2} \leqq \frac{-2(4P-1)^{\frac{1}{2}}}{1 + 4y_{n+1}^2}\left(y_{n+1} - \frac{(4P-1)^{\frac{1}{2}}}{2}\right)\left(y_{n+1} - \frac{1}{2(4P-1)^{\frac{1}{2}}}\right),$$

so that again $\min(y_n, y_{n+1}) \leqq \frac{(4P-1)^{\frac{1}{2}}}{2}$. A similar proof applies to $\Omega_{n+1} = \mp\begin{pmatrix} -a & 1 \\ -P & 0 \end{pmatrix}$.

The second part of the Theorem is obtained immediately from Theorem 5, by taking $\Omega = \begin{pmatrix} 0 & P \\ -1 & 1 \end{pmatrix}$.

20. An application of the preceding results

For complex $z = x + yi$, let

$$t(z) = \frac{(x^2 + y^2)((1 - |x|)^2 + y^2)}{4y^3},$$

and, if ζ is a P-adic integer, define

$$T(\zeta) = \liminf_{n \to \infty} t(z_n).$$

The results in §§17–19 lead to the following

THEOREM 16: *If ζ is rational, then*

$$T(\zeta) = \infty.$$

If ζ is irrational, then for an infinity of indices

$$t(z_n) \leqq \frac{P+1}{4\sqrt{P}},$$

and therefore

$$T(\zeta) \leqq \frac{P+1}{4\sqrt{P}}.$$

Finally, to every $\epsilon > 0$, there is a P-adic integer ζ (which evidently must be irrational), for which

$$\frac{P+1}{4\sqrt{P}} - \epsilon \leqq T(\zeta) \leqq \frac{P+1}{4\sqrt{P}}.$$

PROOF: The first part of the theorem follows immediately from the corollary to Theorem 11, since x_n is bounded.

Now let ζ be irrational. The identity

$$(x^2 + y^2)((1 - |x|)^2 + y^2) - y^2(1 + y^2) = |x|(1 - |x|)\{|x|(1 - |x|) - 2y^2\}$$

shows that for all z in F

$$(x^2 + y^2)((1 - |x|)^2 + y^2) \leqq y^2(1 + y^2),$$

and therefore

$$t(z) \leqq \frac{1 + y^2}{4y}.$$

The function $(1 + y^2)/4y$ has its minimum at $y = 1$, and increases with increasing $|y - 1|$. Hence, by Theorem 12, for an infinity of n

$$t(z_n) \leqq \max\left(\frac{1 + \left(\frac{\sqrt{3}}{2}\right)^2}{4\left(\frac{\sqrt{3}}{2}\right)}, \frac{1 + (\sqrt{P})^2}{4\sqrt{P}}\right) = \frac{P + 1}{4\sqrt{P}},$$

since $(P + 1)/4\sqrt{P}$ increases with P, and

$$\frac{7}{8\sqrt{3}} \leqq \frac{3}{4\sqrt{2}}.$$

The last part of the theorem follows from the proof of Theorem 13, by which, to every $\delta > 0$ there is a P-adic integer ζ such that

$$|z_n - \sqrt{-P}| \leqq \delta$$

for an infinity of n, and

$$y_n \geqq P(\sqrt{P} - \delta)$$

for all other sufficiently large indices. For, if δ is chosen sufficiently small, then for the indices of the first class

$$\left|t(z_n) - \frac{P + 1}{4\sqrt{P}}\right| \leqq \epsilon,$$

and for those of the second class

$$t(z_n) \geqq \frac{y_n}{4} \geqq \frac{P^{3/2}}{4} - \epsilon > \frac{P + 1}{4\sqrt{P}} - \epsilon,$$

as was to be proved.—

For $P \leqq 19$, the expression $(P + 1)/4\sqrt{P}$ is given in the following table:

P	2	3	5	7	11	13	17	19
$(P+1)/4\sqrt{P}$	$\frac{3}{4\sqrt{2}}$	$\frac{1}{\sqrt{3}}$	$\frac{3}{2\sqrt{5}}$	$\frac{2}{\sqrt{7}}$	$\frac{3}{\sqrt{11}}$	$\frac{7}{2\sqrt{13}}$	$\frac{9}{2\sqrt{17}}$	$\frac{5}{\sqrt{19}}$

If ζ satisfies the conditions of Theorem 15, then the upper bound for $T(\zeta)$ can be improved to

$$T(\zeta) \leqq \frac{4P+3}{8(4P-1)^{\frac{1}{2}}},$$

but this is probably not the best possible result.

FINAL REMARK: It is clear that if $f(x, y)$ is an arbitrary function, then the limits

$$\liminf_{n\to\infty} f(x_n, y_n), \qquad \limsup_{n\to\infty} f(x_n, y_n)$$

can be investigated in the same way as for the special cases we have considered. It would be useful to consider in particular the cases $f(x, y) = x/y$ and $f(x, y) = \frac{x^2+y^2}{y}$; the formulae (52) in the next paragraph show why these functions are of interest.

PART II: DIOPHANTINE APPROXIMATIONS IN THE FIELD OF THE P-ADIC NUMBERS

21. Introduction of a binary quadratic form

We shall now use the results of the first part to obtain theorems about *Diophantine Approximations* in the P-adic field. This problem is connected in a very simple way with the properties of the representative $z(\zeta)$ by means of the theory of positive definite binary and ternary quadratic forms.

As usual, if $z = x + yi$ is an arbitrary complex number, we denote its complex conjugate number by a bar: $\bar{z} = x - yi$. Let λ be the same number as in the first part, and $\Phi(X, Y)$ the positive definite binary quadratic form

$$\Phi(X, Y) = \frac{2(X-\lambda Y)(X-\bar{\lambda}Y)}{|\lambda-\bar{\lambda}|} = \mathbf{A}X^2 + 2\mathbf{B}XY + \mathbf{C}Y^2.$$

Obviously its determinant

$$\mathbf{B}^2 - \mathbf{AC} = \frac{(\lambda-\bar{\lambda})^2}{|\lambda-\bar{\lambda}|^2} = -1,$$

and since λ lies in F, Φ is a reduced form. In particular

$$\Phi(X, Y) = X^2 + Y^2, \qquad \text{if } \lambda = i,$$

$$\Phi(X, Y) = \frac{2(X^2+XY+Y^2)}{\sqrt{3}}, \qquad \text{if } \lambda = \frac{-1+\sqrt{-3}}{2}.$$

For $n = 0, 1, 2, \cdots$ put

(49): $$\Phi_n(X, Y) = \Phi(p_nX + p_n'Y, q_nX + q_n'Y) = \mathbf{A}_nX^2 + 2\mathbf{B}_nXY + \mathbf{C}_nY^2,$$

so that the determinant of Φ_n is

(50): $$\mathbf{B}_n^2 - \mathbf{A}_n\mathbf{C}_n = -P^{2n}.$$

By formula (8) in §2,

(51): $$\Phi_n(X, Y) = \mathbf{A}_n(X - z_nY)(X - \bar{z}_nY),$$

and therefore from (50), if $z_n = x_n + y_ni$,

(52): $$\mathbf{A}_n = \frac{P^n}{y_n}, \qquad \mathbf{B}_n = -\frac{P^n x_n}{y_n}, \qquad \mathbf{C}_n = \frac{P^n(x_n^2 + y_n^2)}{y_n}.$$

On the other hand, from (49):

(53): $$\begin{aligned} \mathbf{A}_n &= \Phi(p_n , q_n), \\ \mathbf{B}_n &= \mathbf{A}p_np_n' + \mathbf{B}(p_nq_n' + p_n'q_n) + \mathbf{C}q_nq_n' , \\ \mathbf{C}_n &= \Phi(p_n' , q_n'). \end{aligned}$$

By construction, z_n lies in F. Hence all forms

$$\Phi_n(X, Y) \qquad (n = 0, 1, 2, \cdots)$$

are reduced, so that

(54): $$-\mathbf{A}_n \leqq 2\mathbf{B}_n < \mathbf{A}_n \leqq \mathbf{C}_n , \quad P^{2n} \leqq \mathbf{A}_n\mathbf{C}_n \leqq \tfrac{4}{3}P^{2n}, \quad \mathbf{A}_n \leqq \frac{2}{\sqrt{3}}P^n.$$

Therefore, in particular:

THEOREM 17: *For any P-adic integer ζ and for every positive integer n, there are two integers p_n and q_n, such that*

$$| p_n + q_n\zeta |_P \leqq P^{-n}, \qquad 0 < \Phi(p_n , q_n) \leqq \frac{2}{\sqrt{3}}P^n.$$

22. The P-adic analogue to the Theorem of Lagrange

The following considerations depend on the identity

(55): $$\Phi(p_nX + p_n'Y, q_nX + q_n'Y) = \frac{P^n}{y_n}\{X^2 - 2x_nXY + (x_n^2 + y_n^2)Y^2\},$$

which follows immediately from (52) and (53), and on the inequality

(56): $$| XY' - X'Y |^2 \leqq \Phi(X, Y)\Phi(X', Y'),$$

which is obvious from the identity

$$\begin{aligned} &(\mathbf{AC} - \mathbf{B}^2)(XY' - X'Y)^2 \\ &\qquad = \Phi(X, Y)\Phi(X', Y') - \{\mathbf{A}XX' + \mathbf{B}(XY' + X'Y) + \mathbf{C}YY'\}^2. \end{aligned}$$

THEOREM 18: *Let ζ be a P-adic integer, $\mathbf{T}_n = \begin{pmatrix} p_n & p_n' \\ q_n & q_n' \end{pmatrix}$ the element of $\mathbf{T}(\zeta)$ with index n, and p, q two integers, such that*

$$| p + q\zeta |_P \leqq P^{-n}, \qquad \Phi(p, q) > 0.$$

Then

$$\Phi(p, q) \geqq \Phi(p_n, q_n),$$

with equality if and only if either

$$|z_n| > 1 \quad \textit{and} \quad p = \eta p_n, \qquad q = \eta q_n, \qquad (\eta = \mp 1),$$

or

$$\left.\begin{aligned} |z_n| = 1, \qquad y_n > \frac{\sqrt{3}}{2} \quad \textit{and} \quad p = \eta p_n, \qquad q = \eta q_n, \quad \textit{or} \\ p = \eta p_n', \qquad q = \eta q_n', \end{aligned}\right\} (\eta = \mp 1),$$

or

$$\left.\begin{aligned} z_n = \frac{-1 + \sqrt{-3}}{2} \quad \textit{and} \quad p = \eta p_n, \qquad q = \eta q_n, \quad \textit{or} \\ p = \eta p_n', \quad q = \eta q_n', \quad \textit{or} \quad p = \eta(p_n - p_n'), \quad q = \eta(q_n - q_n'), \end{aligned}\right\} (\eta = \mp 1).$$

PROOF: Suppose that

$$|p + q\zeta|_P \leqq P^{-n}, \qquad 0 < \Phi(p, q) \leqq \Phi(p_n, q_n).$$

Then, from (56),

$$|pq_n' - p_n'q|^2 \leqq \Phi(p_n, q_n)\Phi(p_n', q_n') \leqq \tfrac{4}{3} P^{2n},$$
$$|p_nq - pq_n|^2 \leqq \Phi(p_n, q_n)\Phi(p_n, q_n) \leqq \tfrac{4}{3} P^{2n},$$

while on the other hand

$$|pq_n' - p_n'q|_P$$
$$= |q_n'(p + q\zeta) - q(p_n' + q_n'\zeta)|_P \leqq \max(|p + q\zeta|_P, |p_n' + q_n'\zeta|_P) \leqq P^{-n},$$
$$|p_nq - pq_n|_P$$
$$= |q(p_n + q_n\zeta) - q_n(p + q\zeta)|_P \leqq \max(|p_n + q_n\zeta|_P, |p + q\zeta|_P) \leqq P^{-n}.$$

Therefore each of the two numbers

$$X = \frac{pq_n' - p_n'q}{p_nq_n' - p_n'q_n} \quad \text{and} \quad Y = \frac{p_nq - pq_n}{p_nq_n' - p_n'q_n}$$

is equal either to 0, or to $+1$, or to -1. Now obviously

$$p = p_nX + p_n'Y, \qquad q = q_nX + q_n'Y,$$

so that one of the following four cases occur, where $\eta = \mp 1$:

a) $p = \eta p_n$, $\quad q = \eta q_n$. b) $p = \eta p_n'$, $\quad q = \eta q_n'$.

c) $p = \eta(p_n + p_n')$, $\quad q = \eta(q_n + q_n')$. d) $p = \eta(p_n - p_n')$, $\quad q = \eta(q_n - q_n')$.

The first case is trivial. In case b), from (52),

$$\Phi(p, q) = \Phi(p'_n, q'_n) = \frac{P^n(x_n^2 + y_n^2)}{y_n} \leqq \Phi(p_n, q_n) = \frac{P^n}{y_n},$$

so that necessarily $| z_n | = 1$. In case c), from (55),

$$\Phi(p, q) = \Phi(p_n + p'_n, q_n + q'_n) = \frac{P^n(1 - 2x_n + x_n^2 + y_n^2)}{y_n} \leqq \Phi(p_n, q_n) = \frac{P^n}{y_n},$$

which is impossible for all points z_n in F. Finally in case d), from (55),

$$\Phi(p, q) = \Phi(p_n - p'_n, q_n - q'_n) = \frac{P^n(1 + 2x_n + x_n^2 + y_n^2)}{y_n} \leqq \Phi(p_n, q_n) = \frac{P_n}{y_n},$$

which requires that $z_n = \dfrac{-1 + \sqrt{-3}}{2}$.

23. P-adic analogues to the Theorem of Hurwitz-Borel

The results in §§12–16, the formulae in the last two paragraphs, and Theorem 18 give immediately the following theorems, which form improvements on Theorem 17:

THEOREM 19: A) *To every diadic integer ζ and for at least one of any three consecutive indices n, there are two integers p_n , q_n , for which*

$$| p_n + q_n\zeta |_2 \leqq 2^{-n}, \qquad 0 < \Phi(p_n , q_n) \leqq \frac{2}{\sqrt{7}} \cdot 2^n.$$

B) *To every $\epsilon > 0$, there is a diadic integer ζ, such that*

$$| p + q\zeta |_2 \leqq 2^{-n}, \qquad 0 < \Phi(p, q) \leqq \left(\frac{2}{\sqrt{7}} - \epsilon\right) \cdot 2^n$$

has no integer solution p, q for sufficiently large n.

THEOREM 20: A) *To every triadic integer ζ and for at least one of any three consecutive indices n, there are two integers p_n , q_n , for which*

$$| p_n + q_n\zeta |_3 \leqq 3^{-n}, \qquad 0 < \Phi(p_n , q_n) \leqq \frac{1}{\sqrt{2}} \cdot 3^n.$$

B) *To every $\epsilon > 0$, there is a triadic integer ζ, such that*

$$| p + q\zeta |_3 \leqq 3^{-n}, \qquad 0 < \Phi(p, q) \leqq \left(\frac{1}{\sqrt{2}} - \epsilon\right) \cdot 3^n$$

has no integer solution p, q for sufficiently large n.

THEOREM 21: A) *To every pentadic integer ζ and for at least one of any two consecutive indices n, there are two integers p_n , q_n , for which*

$$| p_n + q_n\zeta |_5 \leqq 5^{-n}, \qquad 0 < \Phi(p_n , q_n) \leqq 5^n.$$

B) *To every* $\epsilon > 0$, *there is a pentadic integer* ζ, *such that*

$$| p + q\zeta |_5 \leqq 5^{-n}, \qquad 0 < \Phi(p, q) \leqq (1 - \epsilon) \cdot 5^n$$

has no integer solution p, q *for sufficiently large* n.

THEOREM 22: *If* $P \equiv 1 \pmod 6$, *then to every* $\epsilon > 0$ *there is a* P*-adic integer* ζ, *such that*

$$| p + q\zeta |_P \leqq P^{-n}, \qquad 0 < \Phi(p, q) \leqq \left(\frac{2}{\sqrt{3}} - \epsilon\right) \cdot P^n$$

has no integer solution p, q *for sufficiently large* n.

Probably for any prime number P and for any P-adic integer ζ

$$\liminf_{n \to \infty} \min_{\substack{| p + q\zeta |_P \leqq P^{-n} \\ \Phi(p,q) > 0}} \frac{\Phi(p, q)}{P^n} \leqq \frac{1}{Y(P)},$$

where $Y(P)$ is the arithmetical function defined in §11; but so far I could prove this only for $P \leqq 7$. That $1/Y(P)$ cannot, in general, be replaced by any smaller number, follows from Theorem 7.

24. The P-adic analogue to the Theorem of Khintchine

The results in §§18–19, the formulae in §21, and Theorem 18 lead immediately to the following results:

THEOREM 23: A) *To every irrational* P*-adic integer* ζ *there is an infinity of indices* n *for which the conditions*

$$| p + q\zeta |_P \leqq P^{-n}, \qquad 0 < \Phi(p, q) < \frac{P^n}{\sqrt{P}}$$

have no integer solution p, q.

B) *To every* $\epsilon > 0$, *there is an irrational* P*-adic integer* ζ, *such that for all sufficiently large* n *there are two integers* p_n, q_n, *for which*

$$| p_n + q_n\zeta |_P \leqq P^{-n}, \qquad 0 < \Phi(p_n, q_n) \leqq \left(\frac{1}{\sqrt{P}} + \epsilon\right) P^n,$$

while for an infinity of indices

$$| p_n + q_n\zeta |_P = P^{-n}, \qquad \frac{P^n}{\sqrt{P}} \leqq \Phi(p_n, q_n) \leqq \left(\frac{1}{\sqrt{P}} + \epsilon\right) P^n.$$

THEOREM 24: A) *If an infinity of elements of* $\Omega(\zeta)$ *belong to* $M'(P)$, *but are different from* $\mp \begin{pmatrix} 0 & P \\ -1 & 0 \end{pmatrix}$, *then there is an infinity of indices* n *for which the inequalities*

$$| p + q\zeta |_P \leqq P^{-n}, \qquad 0 < \Phi(p, q) < \frac{2P^n}{(4P - 1)^{\frac{1}{2}}}$$

have no integer solution p, q.—

B) *To every* $\epsilon > 0$, *there is a P-adic integer* ζ *with the last property, such that for all sufficiently large n there are two integers* p_n, q_n, *for which*

$$|p_n + q_n\zeta|_P \leqq P^{-n}, \qquad 0 < \Phi(p_n, q_n) \leqq \left(\frac{2}{(4P-1)^{\frac{1}{2}}} + \epsilon\right)\cdot P^n.$$

25. The P-adic analogue to the Theorem of Tchebycheff

Ch. Hermite proved the following theorem:[10]

THEOREM 25: *Let*

$$\varphi(X, Y) = AX^2 + 2BXY + CY^2$$

be a reduced positive definite quadratic form, X_0 *and* Y_0 *two real numbers. Then there are two integers X and Y, such that*

$$\varphi(X - X_0, Y - Y_0) \leqq \frac{AC(A - 2|B| + C)}{4(AC - B^2)}.$$

By means of this lemma and the results in §20, we shall prove:

THEOREM 26: *Let* ζ *and* ϑ *be two P-adic integers, of which* ζ *is irrational. Then there is an infinity of indices n, for which there are two integers* u_n *and* v_n, *such that*

$$|u_n + v_n\zeta + \vartheta|_P \leqq P^{-n}, \qquad \Phi(u_n, v_n) \leqq \frac{P+1}{4\sqrt{P}}\cdot P^n.$$

PROOF: For every index n let E_n be the integer defined by

$$|\vartheta - E_n|_P \leqq P^{-n}, \qquad 0 \leqq E_n \leqq P^n - 1.$$

By Theorem 25, there are two integers X_n and Y_n, such that

$$\Phi(p_nX_n + p_n'Y_n - E_n, q_nX_n + q_n'Y_n) \leqq \frac{\mathbf{A}_n\mathbf{C}_n(\mathbf{A}_n - 2|\mathbf{B}_n| + \mathbf{C}_n)}{4(\mathbf{A}_n\mathbf{C}_n - \mathbf{B}_n^2)},$$

since

$$\Phi(p_nX + p_n'Y, q_nX + q_n'Y) = \Phi_n(X, Y) = \mathbf{A}_nX^2 + 2\mathbf{B}_nXY + \mathbf{C}_nY^2$$

is a reduced positive definite form. Obviously, from (52),

$$\frac{\mathbf{A}_n\mathbf{C}_n(\mathbf{A}_n - 2|\mathbf{B}_n| + \mathbf{C}_n)}{4(\mathbf{A}_n\mathbf{C}_n - \mathbf{B}_n^2)} = P^n\,\frac{(x_n^2 + y_n^2)((1 - |x_n|)^2 + y_n^2)}{4y_n^3} = P^n t(z_n);$$

hence, by Theorem 16, for an infinite sequence of indices n

$$\Phi(p_nX_n + p_n'Y_n - E_n, q_nX_n + q_n'Y_n) \leqq \frac{P+1}{4\sqrt{P}}\cdot P^n.$$

[10] Hermite, l. c. 6, 94–99.

Now put

$$v_n = q_n X_n + q_n' Y_n , \qquad w_n = r_n X_n + r_n' Y_n , \qquad u_n = P^n w_n - A_n v_n - E_n ,$$

where A_n , r_n , r_n' are defined as in §§1–2. Since

$$p_n = P^n r_n - A_n q_n , \qquad p_n' = P^n r_n' - A_n q_n' ,$$

obviously

$$u_n = P^n(r_n X_n + r_n' Y_n) - A_n(q_n X_n + q_n' Y_n) - E_n = p_n X_n + p_n' Y_n - E_n ,$$

and therefore

$$\Phi(u_n , v_n) \leqq \frac{P+1}{4\sqrt{P}} P^n .$$

On the other hand

$$u_n + A_n v_n + E_n = P^n w_n , \quad \text{i.e.} \quad | u_n + \zeta v_n + \vartheta |_P \leqq P^{-n},$$

so that u_n and v_n have the required properties.—

If $\Omega(\zeta)$ contains an infinity of elements of $M'(P)$ different from $\mp\begin{pmatrix} 0 & P \\ -1 & 0 \end{pmatrix}$, then the constant $(P+1)/4\sqrt{P}$ in the last theorem can be replaced by the smaller number $(4P+3)/4(4P-1)^{\frac{1}{2}}$. It is nearly certain that both these constants are not the best possible ones; so far, however, I have not been able to obtain the true values.

UNIVERSITY OF MANCHESTER,
MANCHESTER, ENGLAND.