Applications of the theory of elliptic functions in number theory

T. Harmoussis

APPLICATIONS OF THE THEORY OF ELLIPTIC FUNCTIONS IN NUMBER THEORY

M.Sc. Thesis

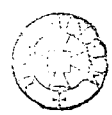
submitted to the

University of Durham

by

T. Harmoussis

University of Durham September 1984



ACKNOWLEDGEMENTS

This M.Sc. thesis has been made under the supervision of Dr. S.M.J. Wilson. His constructive comments and criticisms have been greatly appreciated. I take this opportunity to thank him.

I also wish to express warm thanks to Miss Susan Alcock who has typed my work with real artistry.

I am grateful to my friends at Benton Lodge for their courtesy and also for affording me the opportunity of listening to Dire Straits on lonely nights.

Finally, there are no words to express my feelings to Sotiria who is patiently waiting for me to return home.

T. Harmoussis

. . . . .

. . . . . .

"Της Σαλονίκης μοναχά της πρέπει το καράβι .
Να μην τολμήσεις να τη δείς ποτε απο τη στεριά .
Κι' αν κάποια στην Καλαμαριά πουκάμισο μου ράβει
μπορεί να ρθω απ τα πέλαγα με τη φυρονεριά . "

(Απο το "Τραβέρσο" του Νίκου Καββαδία)

To those who are waiting for me .....

APPLICATIONS OF THE THEORY OF ELLIPTIC FUNCTIONS IN NUMBER THEORY

M.Sc. Thesis
by
T. Harmoussis

ABSTRACT

The aim of this thesis is to present some striking applications of Number Theory, essentially based on the powerful machinery of Elliptic Modular Functions and Class Field Theory.

One of these applications is the explicit determination of all imaginary quadratic fields with class-number one, famous as the 10th discriminant problem. In my discussion of this problem, I have followed the work of K. Heegner and others, based on the results of H. Weber found in his "Lehrbuch der Algebra". I have presented the results of Weber adopting up to date methods, since Weber's proofs were rather computational using complicated, lengthily presented properties of theta functions. For this purpose I have been rescued by Group Theory, which has been used throughout to prove the critical results of Weber. Thus, I have shortened the ground work which I needed for further exploration.

A second application very closely related to the above is the identification of elliptic curves with infinitely many rational points, or, what is essentially the same thing, cubic equations with infinitely many rational solutions.

In the first part of this work I have provided a systematic development of a pertinent background for the objectives outlined above.

CONTENTS

B. ELLIPTIC FUNCTIONS AND ELLIPTIC CURVES

CHAPTER II

THE APPLICATION OF MODULAR FUNCTIONS IN TO THE CLASS FIELD THEORY OF IMAGINARY QUADRATIC FIELDS

CHAPTER III

THE DETERMINATION OF ALL

IMAGINARY QUADRATIC FIELDS

WITH CLASS NUMBER ONE

CHAPTER IV

ELLIPTIC CURVES WITH

INFINITELY MANY

RATIONAL POINTS

REFERENCES

INTRODUCTION

This thesis is naturally divided into two parts. The first is concerned with establishing an appropriate background necessary for our purposes and this occupies the first two chapters. The second part, the last two chapters, deals with two remarkable applications in Number Theory: the Gauss 10th discriminant problem and the discovery of an infinite series of Elliptic Curves each with infinitely many rational points.

Chapter I is of an introductory nature and is divided into two sections, A. MODULAR FUNCTIONS and B. ELLIPTIC FUNCTIONS AND ELLIPTIC CURVES.

The first is concerned with the Modular Group, Modular Functions and Modular Forms. In paragraphs 1, 2 and 3 we review briefly this beautiful area of Mathematics treating in particular the concept of level of a subgroup of the Modular Group and the cusps of principal congruence subgroups. It now seems to me, having had the opportunity to attend the the recent International Symposium on Modular Forms at Durham, that this subject offers a whole range of fascinating conjectures.

In paragraph 4 we give a detailed exposition of some Modular Functions which constitute the main ingredients of our work. In particular we examine the properties of Weber's functions f, f_1 and f_2 . Birch and Heegner (as we point out) use these functions (or very similar ones) with conflicting notation. Both for historical reasons and for the sake of clarity we stick to Weber's notation and definitions. Therefore we have set ourselves the challenging task of presenting proofs of all properties of the Weber functions which we need. The Theorem I. 4.6.10, in its extended form, has been one of the most interesting statements to prove.

Paragraph 5 rapidly presents the necessary preliminaries on the Modular polynomial in order to prove at the end three significant theorems.

The section B of Chapter I introduces the most basic properties of Elliptic Functions and Elliptic Curves, including the Addition Theorem, the possibility of complex multiplication and the Mordell-Weil Theorem. I have found three excellent surveys of this subject (see Cassels [10] , Tate [47] , and Gelbart [18]), which should be mentioned here. I have also tried to avoid too great a generality, as too much Algebraic geometry would have taken us beyond the intended scope of our thesis. Lang says: "It is possible to write endlessly on elliptic curves".

In Chapter II we look at the application of Modular Functions to the Class Field Theory of imaginary quadratic fields. Our principal aims are a statement of the Söhngen theorem and a closer examination of the case where the discriminant $D = -p$, $P \equiv 3 \pmod 4$ and p is a prime greater than 3.

Chapter III is devoted to the longstanding Gauss' conjecture that there are exactly 9 imaginary quadratic fields with class-number, h(-p) is equal to 1 (given by $p = 3, 4, 7, 8, 11, 19, 43, 67, 163$).

In 1951 Heegner (see [23]) was motivated by a lemma of Weber (see [48] , § 125) stated as follows: "If p is a rational prime $\equiv 3 \pmod 8$, and h(-p) = 1, then $\gamma_2\left(\frac{-3+\sqrt{-p}}{2}\right)$ is a rational integer" to prove the Gauss conjecture. When his proof appeared it was discounted, because it was thought that the proof was based on a conjecture of Weber that had not been proved at the time. Using our notation Heegner's proof was based on a fact, actually proved by Weber, that

$$e^{3\pi i/4} f_2^6(\omega) \in K_2$$

and not on Weber's conjecture

$$\sqrt{2}\, e^{-\pi i/8} f_2^3(\omega) \in K_2$$

(which has subsequently been proved by Birch [4]).
Indeed the ideas of Heegner are effective not only for the class-number problem but also for the study of rational points on Elliptic Curves.

Historically, the first generally accepted proofs were given by Stark (see [45]) and Baker (see [3]) in 1967. They have also showed, by using a transcendence theorem, that there are exactly 18 imaginary quadratic fields with class-number two. Recently great progress has been made on bounding the class-number of quadratic fields in general (se e.g. [19] , [24]).

Chapter IV is devoted to elliptic curves defined over the rationals with infinitely many rational points. This fascinating subject involves inevitably a certain amount of Algebraic Geometry. Siegel proved (see [42]) that on an arbitrary affine curve of genus $\geqslant 1$ there exist only a finite number of integral points. The question of whether there exists a rational point is extremely difficult, and there is as yet no known procedure for deciding in general. Reichardt showed that there are no rational points on $x^4 - 17 = 2y^2$. Birch (see [5]) has presented a family of Elliptic curves defined over the rationals such that each of these curves has infinitely many rational points.

All definitions, theorems, and remarks within a single chapter are numbered consecutively. Bibliographical references are given by numbers enclosed in square brackets.

CHAPTER I
PRELIMINARIES

A. MODULAR FUNCTIONS

1. Standard Notation - Lattices in the complex plane

We denote by $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ the ring of rational integers, the field of rational numbers, the field of real numbers, the field of complex numbers, respectively.

We also denote by:

$\bar{\mathbb{C}} := \mathbb{C} \cup \{i\infty\}$

$\mathfrak{H} := \{z \in \mathbb{C} : Im(z) > 0\}$, the upper half of the complex plane

$\mathfrak{H}^* := \mathfrak{H} \cup \{i\infty\} \cup \mathbb{Q}$

For a commutative ring R with unity, we denote by $R^\times$ the group of units of R, and by $M_2(R)$ the ring of all 2 x 2 matrices with entries in R.

Now we set:

$GL_2(R) = M_2(R)^\times$

$SL_2(R) = \{A \in GL_2(R) : \det(A) = 1\}$

Finally, we denote by $\hat{\Gamma}$ the quotient group $SL_2(\mathbb{Z})/\{\pm I\}$,

where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Note that $\hat{\Gamma}$ acts on $\mathfrak{H}$, on the left, by Möbius transformations, in the obvious way.

Definition (Def I,1,1)

Let V be a real vector space of finite dimension n .

A (full) lattice L in V is a discrete subgroup of V of rank n, in other words, an additive subgroup of V generated by a basis of V .

Regarding the complex plane as a two-dimensional vector space

over the reals, a lattice L in the complex plane is a freely generated subgroup of $\mathbb{C}$ of rank 2, that is, there are $\omega_1, \omega_2 \in \mathbb{C}$ with $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$, so that:

$$L = [\omega_1, \omega_2] = \{ m\omega_1 + n\omega_2 : m, n \in \mathbb{Z} \}$$

In the following we keep fixed the notations:

$L = [\omega_1, \omega_2]$ for a lattice in the complex plane with $jm(\frac{\omega_1}{\omega_2}) > 0$, and, putting $\tau = \frac{\omega_1}{\omega_2}$, we denote by $\Lambda = [\tau, 1]$ the normalized lattice.

Now we make some important remarks on lattices in the complex plane:

Remark (Rem. I. 1.2)

It is easily seen that the pairs (ω_1, ω_2), (ω_1', ω_2') with entries in $\mathbb{C}^*$ generate the same lattice in $\mathbb{C}$, if and only if, they are equivalent with respect to $GL_2(\mathbb{Z})$, in other words, if and only if, there is a unimodular integer matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that:

$$\begin{Bmatrix} \omega_1' \\ \omega_2' \end{Bmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{Bmatrix} \omega_1 \\ \omega_2 \end{Bmatrix} .$$

We denote by:

$\mathcal{L}$, the set of all latices in $\mathbb{C}$, and

$\mathcal{M}$, the set of all pairs (ω_1, ω_2) with entries in $\mathbb{C}^*$, such that $jm(\frac{\omega_1}{\omega_2}) > 0$.

Remark (Rem. I. 1.3)

The group $SL_2(\mathbb{Z})$ acts on $\mathcal{M}$, on the left in the obvious way:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} . \quad (\omega_1, \omega_2) = (a\omega_1 + b\omega_2 , c\omega_1 + d\omega_2).$$

The action is well defined, since

$$jm\left(\frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2}\right) = \frac{jm(\frac{\omega_1}{\omega_2})}{\left| c\frac{\omega_1}{\omega_2} + d \right|^2} > 0$$

Thus, the quotient $\mathcal{M}/SL_2(\mathbb{Z})$ is identified with $\mathcal{L}$, by the map

$$(\omega_1, \omega_2) \longmapsto [\omega_1, \omega_2]$$

Now, the group $\mathbb{C}^*$ acts on $\mathcal{M}$ (resp. on $\mathcal{L}$) by:

$$\lambda\cdot(\omega_1,\omega_2)=(\lambda\omega_1,\lambda\omega_2)\quad\left(\text{resp. }\lambda[\omega_1,\omega_2]=[\lambda\omega_1,\lambda\omega_2]\right)\ .$$

The quotient $\mathcal{M}/\mathbb{C}^*$ is identified with $\mathcal{H}$, by the map

$$(\omega_1,\omega_2)\longmapsto\tau=\frac{\omega_1}{\omega_2}$$

and since this identification transforms the action of $SL_2(\mathbb{Z})$ on $\mathcal{M}$ into that of $\hat{\Gamma}$ on $\mathcal{H}$, we have that :

Remark (Rem. I. 1.4)

There is a bijection of $\mathcal{L}/\mathbb{C}^*$ onto $\mathcal{H}/\Gamma$ induced by the map

$$(\omega_1,\omega_2)\longmapsto\tau=\frac{\omega_1}{\omega_2}\ .$$

The basic functions we shall be dealing with are the Eisenstein functions g_2, g_3, the discriminant Δ, the Klein function J, and the absolute invariant j.

For our given lattice $L=[\omega_1,\omega_2]$ the Eisenstein series of order $2n$, $n\geqslant 2$ is given by

$$G_n(L)=\sum_{\substack{\omega\in L\\ \omega\neq 0}}\frac{1}{\omega^{2n}}\ .$$

We make the following definitions:

$$g_2(L)=60G_2(L)$$

$$g_3(L)=140G_3(L)$$

$$\Delta(L)=g_2^3(L)-27g_3^2(L)$$

$$J(L)=\frac{g_2^3(L)}{\Delta(L)}$$

$$j(L)=1728\,J(L)\ .$$

In terms of the normalised lattice $\Lambda=[\tau,1]$ we have

$$G_n(\Lambda)=\sum_{(c,d)\neq(0,0)}\frac{1}{(c\tau+d)^{2n}}\ ,\quad n\geqslant 2 \tag{I.1.5}$$

$$g_2(\Lambda)=60G_2(\Lambda) \tag{I.1.6}$$

$$g_3(\Lambda)=140\,G_3(\Lambda) \tag{I.1.7}$$

$$\Delta(\Lambda)=g_2^3(\Lambda)-27g_3^2(\Lambda) \tag{I.1.8}$$

$$J(\Lambda)=\frac{g_2^3(\Lambda)}{\Delta(\Lambda)} \tag{I.1.9}$$

$$j(\Lambda)=1728\,J(\Lambda) \tag{I.1.10}$$

2. THE MODULAR GROUP

2.1 General Facts and Definitions

The homogeneous modular group $\Gamma(1)$ is defined to be the group $SL_2(\mathbb{Z})$

Note that, for each $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$ corresponds a Möbius transformation $T: \bar{\mathbb{C}} \longrightarrow \bar{\mathbb{C}}$, given by

$$T(z) = \frac{az+b}{cz+d} \quad .$$

We denote by $\hat{\Gamma}(1)$ the set of all Möbius transformations defining by the elements of $\Gamma(1)$. The set $\hat{\Gamma}(1)$ turns out to be a group under the composition of mappings, and is called the inhomogeneous modular group.

The map: $\phi : \Gamma(1) \longrightarrow \Gamma(1)$ defined by:

$$\phi(T) = T \quad \forall T \in \Gamma(1)$$

is clearly a group epimorphism with $\text{Ker}(\phi) = \{I, I\}$, where I is the identity matrix.

Therefore we have:

$$\Gamma(1)/\{\pm I\} \cong \hat{\Gamma}(1)$$

Let G be any subgroup of $\Gamma(1)$. We denote by $\hat{G}$ the inhomogeneous image of G under ϕ.

Note that:

if $-I \in G$, then $G/\{\pm I\} \cong \hat{G}$

and if $-I \notin G$, then $G \cong \hat{G}$.

Definition (Def I.2 1.1)

The Modular group $\hat{\Gamma}$ is defined to be the inhomogeneous modular group $\hat{\Gamma}(1)$, although we may prefer to think of it as the quotient group $\Gamma(1)/\{\pm I\}$, or indeed as the homogeneous group $\Gamma(1)$, with every matrix T identified with -T.

The theory of row reduction of integral matrices shows that the Modular group $\hat{\Gamma}$ is generated by the elements S, T given by:

$$S : \tau \longmapsto -\frac{1}{\tau} \quad , \quad T : \tau \longmapsto \tau + 1 \quad .$$

Clearly therefore $\hat{\Gamma}$ is also generated by the elements S, ST, which are of order 2,3 respectively. In fact, it can be proved that $\hat{\Gamma}$ is the free product

$$\hat{\Gamma} = \langle S \rangle * \langle ST \rangle \quad .$$

2.2 The Action of $\hat{\Gamma}$ on $\mathfrak{H}^*$

The modular group $\hat{\Gamma}$ acts on $\mathfrak{H}^*$ in the usual way

$$\gamma.\tau = \gamma(\tau) \qquad \forall\, \gamma \in \hat{\Gamma}\,, \forall\, \tau \in \mathfrak{H}^*$$

In particular, if γ is the inhomogeneous image of the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$, then we have:

Remark (Rem I 2.2.1)

(i) $\gamma(\tau) \in \mathfrak{H}\ \forall\, \tau \in \mathfrak{H}$, since $\operatorname{jm}\left(\frac{a\tau + b}{c\tau + d}\right) = \frac{\operatorname{jm}(\tau)}{|c\tau + d|^2}$

(ii) $\gamma(i\infty) = \begin{cases} a/c & , \text{ if } c \neq 0 \\ i\infty & , \text{ if } c = 0 \end{cases}$

(iii) For $\tau = q \in \mathbb{Q}$

$$\gamma(q) = \begin{cases} q + \frac{b}{d} & , \text{if} \quad c = 0 \\ \frac{aq+b}{cq+d} & , \text{if} \quad c \neq 0 \quad , \quad q \neq -\frac{d}{c} \\ i\infty & , \text{if} \quad c \neq 0 \quad , \quad q = -\frac{d}{c} \end{cases}$$

Definitions (Def. I 2.2.2.)

A fundamental set of $\hat{\Gamma}$, for $\mathfrak{H}^*$, is defined to be any subset of $\mathfrak{H}^*$ containing just one point of each orbit.

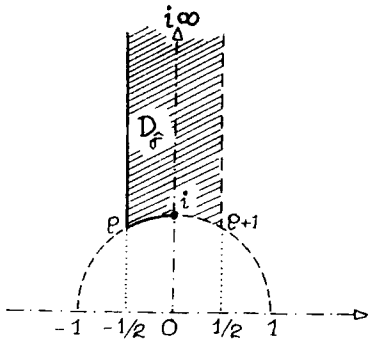
A fundamental domain of $\hat{\Gamma}$, for $\mathfrak{H}^*$, is defined to be a set containing a fundamental set of $\hat{\Gamma}$, for $\mathfrak{H}^*$, and if it contains two points of the sameorbit, then they lie on the boundary.

Theorem (Th. I. 2.2.3) (See Schoeneberg [37] , p.p. 17, Th. 13)

The Set $D_{\hat{\Gamma}} = \left\{\tau \in \mathfrak{H} : |\mathrm{Re}(\tau)| < \frac{1}{2}\,,\ |\tau| > 1\right\} \cup \{i\infty\}$

$$\cup \left\{\tau \in \mathfrak{H} : \mathrm{Re}(\tau) = -\tfrac{1}{2}\,,\ |\tau| \geq 1\right\} \cup \left\{\tau \in \mathfrak{H} : |\tau| = 1\,,\ -\tfrac{1}{2} \leq \mathrm{Re}(\tau) < 0\right\}$$

is a fundamental domain of $\hat{\Gamma}$ for $\mathfrak{H}^*$.



The boundary of $D_{\hat{\Gamma}}$ consists of pairs of equivalent sides, namely:

The vertical sides $(p, i\infty) \sim (p+1, i\infty)$, which are mapped one onto the other by the transformations T or T^{-1}, and the arc sides $(p, i) \sim (p+1, i)$ which are mapped one onto the other by the transformation S.

Let $\hat{\Gamma}_\tau = \{\gamma \in \hat{\Gamma} : \gamma(\tau) = \tau\}$ be the stabilizer of an element $\tau \in D_{\hat{\Gamma}}$ under $\hat{\Gamma}$. Then one has:

$\hat{\Gamma}_{i\infty} = \langle T \rangle$, infinite cyclic group, generated by T .

$\hat{\Gamma}_i = \langle S \rangle$, cyclic group of order 2, generated by S .

$\hat{\Gamma}_\rho = \langle ST \rangle$, cyclic group of order 3, generated by ST .

In all other cases of $\tau \in D_{\hat{\Gamma}}$, $\hat{\Gamma}_\tau = \{1_d\}$.

Therefore every element $\gamma \in \hat{\Gamma}$ is uniquely determined by the image of a point $\tau \in D_{\hat{\Gamma}}$, distinct from $i\infty, \rho, i$.

It is easy to deduce from the (def. I. 2.2.2) the following:

Remark (Rem I.2.2.4)

The map $D_{\hat{\Gamma}} \longrightarrow \mathfrak{H}^*/\hat{\Gamma}$, defined by $\tau \longmapsto \text{orbit}_{\hat{\Gamma}}(\tau)$, is bijective. In particular, this map sends

$$i\infty \longmapsto \{i\infty\} \cup \mathbb{Q}$$

since $\text{orbit}_{\hat{\Gamma}}(i\infty) = \{i\infty\} \cup \mathbb{Q}$.

Theorem (Th. I 2.2.5)

(i) Let $(c, d) = 1$

Then every element of $\hat{\Gamma}$ sending $-\frac{d}{c}$ to $i\infty$ is of the form $T^k L$, $k \in \mathbb{Z}$, where L is the inhomogeneous image of matrix $L = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

(ii) Let $(c, d) = (c_1, d_1) = 1$

Then every element of $\hat{\Gamma}$ sending $-\frac{d}{c}$ to $-\frac{d_1}{c_1}$ is of the form $L_1^{-1} T^k L$, $k \in \mathbb{Z}$,

where L, L_1 are the inhomogeneous images of matrices, $L = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $L_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$, of $\Gamma(1)$, respectively.

Proof

(i) Suppose that V is a matrix lying in $\Gamma(1)$ whose the inhomogeneous image, V say, is such that

$$V\left(-\frac{d}{c}\right) = i\infty$$

Then $V = \begin{pmatrix} x & y \\ c & d \end{pmatrix}$.

Since (c,d) = 1, the Diophantine equation $dx - cy = 1$ has solution $x = a + kc$, $y = b + kd$, where $k \in \mathbb{Z}$.

Therefore $V = T^k L$.

The converse is obvious .

(ii) Let $V \in \hat{\Gamma}$, and $V\left(-\frac{d}{c}\right) = -\frac{d_1}{c_1}$

Then for an arbitrary integer K_1 we have

$$T^{K_1} L_1 V \left(-\frac{d}{c}\right) = T^{K_1} L_1 \left(\frac{d_1}{c_1}\right) = i\infty ,$$

since (i) .

Therefore $T^{K_1} L_1 V = T^{K_2} L$ for some integer K_2 .

Hence $V = L_1^{-1} T^K L$, $K \in \mathbb{Z}$.

The converse is obvious .

2.3 Fixed Points for $\hat{\Gamma}$

Let γ be the Möbius transformation, corresponding to the matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$. We find the fixed points of $\mathfrak{H}^*$ by γ .

Case 1, $c \neq 0$

The only possibility for $\gamma(\tau) = \tau$, $\tau \in \mathfrak{H}^*$ is that

$$\frac{a\tau + b}{c\tau + d} = \tau, \text{ and } \tau \in \mathfrak{H}^* \setminus \left\{ i\infty , -\frac{d}{c} \right\}$$

which is equivalent to

$$\tau = \frac{(a - d) \pm \sqrt{(a + d)^2 - 4}}{2c} \quad , \text{ and } \quad |\mathrm{tr}\,(\gamma)| = |a + d| \leq 2 .$$

Suppose $|\mathrm{tr}\,(\gamma)| < 2$ (the elliptic case).

In this case ρ fixes only the point $\tau = \dfrac{(a-d)+\sqrt{(a+d)^2-4}}{2c}$ lying on $\mathfrak{H}$.

Every element $\rho \in \hat{\Gamma}$ such that: $|tr(\rho)| < 2$ is called elliptic, and by the above, every elliptic transformation fixes only one point of $\mathfrak{H}^*$ lying on the upper half plane.

Using standard thorems of integral matrices, one proves that an elliptic element of $\hat{\Gamma}$ is either of order 2 and is of the form $L^{-1} S L$, for some $L \in \hat{\Gamma}$, or, is of order 3 and is of the form $L^{-1}(ST)^K L$, where $K = 1$ or 2, for some $L \in \hat{\Gamma}$.

Now, if $\tau \in \mathfrak{H}^*$ is a fixed point for an elliptic element ρ of order 2, then

$$L^{-1} S L (\tau) = \tau, \text{ for some } L \in \hat{\Gamma}.$$

and therefore $SL(\tau) = L(\tau)$, which means that $L(\tau)$ is a fixed point for S. Since the only fixed point of $\mathfrak{H}$ for S is i, we deduce that $L(\tau) = i$, that is $\tau = L^{-1}(i)$.

We denote by $E_2 = \{ L^{-1}(i) : L \in \hat{\Gamma} \}$ the set of all elliptic fixed points of order 2 in $\mathfrak{H}$.

Similarly, one proves that $E_3 = \{ L^{-1}(\rho) : L \in \hat{\Gamma} \}$ is the set of all elliptic fixed points of order 3 in $\mathfrak{H}$, where $\rho = e^{2\pi i/3}$.

Suppose, now, $|tr(\rho)| = 2$

In this case, ρ fixes only the rational number $\dfrac{a-d}{2c}$.

Case 2, $c = 0$

In this case $a = d = \pm 1$, and so if the matrix $\rho \neq \pm I$, the transformation ρ fixes only the point at infinity. Any element $\rho \in \hat{\Gamma}$ with matrix $\rho \neq \pm I$, and $|tr(\rho)| = 2$ is called parabolic.

Every parabolid element of $\hat{\Gamma}$ fixes only one point of $\mathfrak{H}^*$, which is either a rational number or the point at infinity . Using standard theorems of integral matrices, one proves that a parabolic element of $\hat{\Gamma}$ is of infinite order in $\hat{\Gamma}$ and takes the form $L^{-1} T^K L$, for some $L \in \hat{\Gamma}$, where $K \in \mathbb{Z} \setminus \{0\}$.

Now, if $\tau \in \mathfrak{H}^*$ is a fixed point for a parabolic element ρ then,

$$L^{-1} T^K L (\tau) = \tau, \text{ for some } L \in \hat{\Gamma}, K \in \mathbb{Z} \setminus \{0\}$$

and therefore $T^K L(\tau) = L(\tau)$, which means that $L(\tau)$ is a fixed point for T^K, that is

$$L(\tau) = i\infty$$

and so $\tau = L^{-1}(i\infty)$.

We denote by $\mathbb{P} = \{ L^{-1}(i\infty) : L \in \hat{\Gamma} \}$ the set of all parabolic fixed points which are also called cusps of the modular group $\hat{\Gamma}$.

Summarising the above analysis we see that the elements of the Modular group $\hat{\Gamma}$ acting on the extended upper half plane $\mathfrak{H}$ can be divided into four classes:

1. The identity transformation 1.
2. Elliptic transformations of order 2, which are of the form $L^{-1} S L$, for some $L \in \hat{\Gamma}$.
   Each of them fixes only one point lying on $\mathfrak{H}$, and the set of fixed points is :
   $$E_2 = \{ L^{-1}(i) : L \in \hat{\Gamma} \}.$$
3. Elliptic transformations of order 3, which are of the form $L^{-1}(ST)^K L$, for some $L \in \hat{\Gamma}$, where $k = 1$ or 2.
   Each of them fixes only one point lying on $\mathfrak{H}$, and the set of fixed points is :
   $$E_3 = \{ L^{-1}(\rho) : L \in \hat{\Gamma} \},$$
   where $\rho = e^{2\pi i/3}$.

An elliptic transformation occurs, if and only if the trace of the corresponding matrix has absolute value less than 2.

4. Parabolic transformations, which are of the form $L^{-1} T^K L$, for some $L \in \hat{\Gamma}$, where $K \in \mathbb{Z} \setminus \{0\}$.
   Each of them fixes only one point of $\mathfrak{H}^*$ which is either a rational number or the point at infinity $i\infty$ and the set of fixed parabolic points (cusps) is :
   $$\mathbb{P} = \{ L^{-1}(i\infty) : L \in \hat{\Gamma} \}.$$

Finally, a parabolic transformation occurs, if and only if, the trace of the corresponding matrix is ± 2, and the matrix itself is $\neq \pm I$.

2.4 Subgroups of $\hat{\Gamma}$ of finite index. The concept of level.

Let n be any positive integer.

Set $\Gamma(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) : a \equiv d \equiv 1 \pmod{n},\ b \equiv c \equiv 0 \pmod{n} \right\}$.

It is easy verified that $\Gamma(n)$ is a normal subgroup of $\Gamma(1)$ and in fact, it is the kernel of the natural homomorphism

$\Gamma(1) \longrightarrow SL_2(\mathbb{Z}n)$, which is also onto .

Thus :

$$\Gamma(1)/\Gamma(n) \cong SL_2(\mathbb{Z}_n) \qquad \text{(I. 2.4.1)}$$

The subgroup $\Gamma(n)$ is called the homogeneous principal congruence subgroup of level n.

We write $\hat{\Gamma}(n)$ for the subgroup of $\hat{\Gamma}$ which corresponds to $\Gamma(n)$, and we call it the inhomogeneous principal congruence subgroup of level n.

Since $-I \in \Gamma(n)$, if and only if, n = 1 or 2,

we have:

$$\hat{\Gamma}(n) \cong \Gamma(n)/\{\pm I\} \quad , \quad (n=1,2)$$

$$\hat{\Gamma}(n) \cong \Gamma(n) \quad , \quad (n \geqslant 3) \qquad \text{(I. 2.4.2)}$$

By a simple argument , counting the incongruent solutions of $ad - bc \equiv 1 \pmod{n}$, one proves that the order of $SL_2(\mathbb{Z}_n)$ is $n^3 \prod_{p|n} \left(1 - \frac{1}{p^2}\right)$.

Therefore, setting $\mu(n) = \left[\Gamma(1) : \Gamma(n)\right]$, it follows from (I.2.4.1), that:

$$\mu(n) = n^3 \prod_{p|n} \left(1 - \frac{1}{p^2}\right) \qquad \text{(I.2.4.3)}$$

Also, setting $\hat{\mu}(n) = \left[\hat{\Gamma} : \hat{\Gamma}(n)\right]$, since (I.4.4.2) we have :

$$\hat{\mu}(n) = \mu(n) \quad , \quad (n=1,2)$$

$$\mu(n) = \frac{1}{2}\mu(n) \quad , \quad (n \geqslant 3) \qquad \text{(I. 2.4.4)}$$

Definition (Def. I.2.4.5)

Let G be any subgroup of $\Gamma(1)$.

We say that G is a congruence subgroup of $\Gamma(1)$, if $\Gamma(n) \subseteq G$, for some positive integet n.

The notion of an inhomogeneous congruence subgroup is defined similarly.

We give, now, a short list of some important congruence subgroups:

For a positive integer n, we set:

$$\Gamma_0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) : \quad c \equiv 0 \pmod{n} \right\}$$

$$\Gamma^0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) : \quad b \equiv 0 \pmod{n} \right\}$$

$$\Gamma_0^0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) : \quad b \equiv c \equiv 0 \pmod{n} \right\}$$

We set: $$\psi(n) = \left[\Gamma(1) : \Gamma_0(n)\right] = \left[\Gamma(1) : \Gamma^0(n)\right] ,$$

$$\hat{\psi}(n) = \left[\hat{\Gamma} : \hat{\Gamma}_0(n)\right] = \left[\hat{\Gamma} : \hat{\Gamma}^0(n)\right] .$$

Since $$-I \in \Gamma_0(n) \quad , \quad \Gamma_0(n)/\{\pm I\} \cong \hat{\Gamma}_0(n)$$

and therefore $$\psi(n) = \hat{\psi}(n) .$$

Note that, if $c \equiv 0 \pmod{n}$, the congruence $ad - bc \equiv 1 \pmod{n}$ has exactly $n\varphi(n)$ incongruent solutions, where φ is the Euler φ - function. Therefore: $\left[\Gamma_0(n) : \Gamma(n)\right] = n\varphi(n) = n^2 \prod_{p|n} \left(1 - \frac{1}{p}\right)$.

From (I.2.4.3), we deduce that:

$$\psi(n) = n \prod_{p|n} \left(1 + \frac{1}{p}\right) \qquad \text{(I.2.4.6)}$$

and $$\left[\Gamma(1) : \Gamma_0^0(n)\right] = \left[\hat{\Gamma} : \Gamma_0^0(n)\right] = n\psi(n) \qquad \text{(I.2.4.7)}$$

We discuss, now, the notion of <u>the level</u> of a subgroup G of $\Gamma(1)$, in the case, where G is of finite index in $\Gamma(1)$.

Let G be any subgroup of $\Gamma(1)$ of finite index, μ say. Since $\Gamma(1)$ is finitely generated group by S, T, G is also finitely generated. Furthermore, by Schreier's theorem, the number of generators of G does not exceed $1 + \mu$.

Since the matrix T is of infinite order in $\Gamma(1)$, for each $V \in \Gamma(1)$, we are allowed to define n_V to be the least positive integer such that:

$$T^{n_V} \in V G V^{-1}$$

Since G is of finite index in $\Gamma(1)$, the number of conjugate subgroups of G in $\Gamma(1)$ is also finite, and in fact this number is equal to $\left|\Gamma(1)/N_{\Gamma(1)}(G)\right|$, where $N_{\Gamma(1)}(G)$ is the normalizer of G in $\Gamma(1)$. Therefore the set $\{n_V : V \in \Gamma(1)\}$ is finite.

Keeping fixed the above notations, we give the Wohlfahrt (1964) definition of the level of the subgroup G of $\Gamma(1)$.

Definition (Def. I. 2.4.8)

Let G be any subgroup of $\Gamma(1)$, of finite index. The level N of G is defined to be the least common multiple of n_V, $V \in \Gamma(1)$, and write :

$$\text{lev}(G) = N \quad .$$

Let n be any positive integer.

We denoted by $\Delta(n)$ the normal closure of the cyclic group $\langle T^n \rangle$ in $\Gamma(1)$, that is the intersection of all normal subgroups of $\Gamma(1)$, which contain $\langle T^n \rangle$.

Following the standard properties of the normal closure we have:

(i) $\Delta(n)$ is the unique smallest normal subgroup of $\Gamma(1)$ containing $\langle T^n \rangle$, and

(ii) $\Delta(n) = \langle V^{-1} T^n V : V \in \Gamma(1) \rangle$

Thus, if G is a subgroup of $\Gamma(1)$, of finite index, then we may equivalently define the level of G as follows:

Definition (Def I. 2.4.9)

Let G be any subgroup of $\Gamma(1)$, of finite index, and N be any positive integer. We say that G is of level N, if and only if,

$$\Delta(N) \subseteq G \quad ,$$

and N is the smallest positive integer for which this inclusion holds, that is, N is the smallest positive integer, such that:

$$V^{-1} T^N V \in G \qquad \forall V \in \Gamma(1) \ .$$

We make exactly similar definitions for inhomogeneous groups,

which are of finite index in $\hat{\Gamma}$.

Now, it can be easily proved that:

Remark (Rem I. 2.4.10)

$$\text{lev}\left(\Gamma(N)\right) = \text{lev}\left(\hat{\Gamma}(N)\right) = N$$

Suppose, now, that G is a congruence subgroup of $\Gamma(1)$. Therefore $\Gamma(n) \subseteq G$ for some positive integer n, and so G is of finite index in $\Gamma(1)$. Let lev (G) = N, where N is a positive integer, and hence N is the least positive integer such that $VT^N V^{-1} \in G$ for any arbitrary chosen $V \in \Gamma(1)$. So N is the least positive integer such that $T^N \in G$. But, since $\Gamma(n) \in G$ we have also $T^n \in G$ and therefore $N \mid n$. So we have proved the following:

Remark (Rem I.2.4.11)

If $\Gamma(n) \subseteq G \subseteq \Gamma(1)$ for any positive integer n, then

$$\text{lev}\ (G) \mid n \quad .$$

We state now a more general result:

Theorem (Th. I.2.4.12)

Let G be any congruence subgroup of G.

Then lev (G) = N, if and only if, N is the least positive integer such that $\Gamma(N) \subseteq G$.

Proof

Let N_o be the least positive integer such that $\Gamma(N_o) \subseteq G$ (1).

We will prove that $N_o = N$.

By the previous remark, $N \mid N_o$ (2)

Because of (1), and (2), it is enough to prove that $\Gamma(N) \subseteq G$.

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be any element of $\Gamma(N)$.

We reduce A, step by step, in such a way that the result $A \in G$ becomes obvious.

First Step

Since $T^N \in G$, $T^{Nk} \in G$ for any integer K

Note that: $A\,T^{Nk} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & Nk \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & aNk + b \\ c & cNk + d \end{pmatrix}$

Since $(d, N) = (d, c) = 1$, $(d, cN) = 1$.

Therefore choosing any integer k, such that:

$$cNk \not\equiv -d \pmod{\frac{N_o}{N}}$$

we have $(cNk + d, N_o) = 1$.

Thus we may assume that $(d, N_o) = 1$.

Second Step (After the assumption $(d, N_o) = 1$ is made)

Note that: $T^{\lambda N} A = \begin{pmatrix} 1 & \lambda N \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a + cN\lambda & b + dN\lambda \\ c & d \end{pmatrix}$

Since $(d, N_o) = 1$, choosing any integer λ, such that:

$$\frac{b}{N} + d\lambda \equiv 0 \pmod{N_o}$$

we deduce $b + dN\lambda \equiv 0 \pmod{N_o}$.

Thus, we may further assume that $b \equiv 0 \pmod{N_o}$.

Since $\begin{pmatrix} 1 & 0 \\ \mu N & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -\mu N \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ (3)

the matrix $\begin{pmatrix} 1 & 0 \\ \mu N & 1 \end{pmatrix}$ lies in G.

We have also $A\begin{pmatrix} 1 & 0 \\ \mu N & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ \mu N & 1 \end{pmatrix} = \begin{pmatrix} a + bN\mu & b \\ c + dN\mu & d \end{pmatrix}$

Since $(d, N_o) = 1$, we can choose an integer μ, such that

$$c + dN\mu \equiv 0 \pmod{N_o} .$$

Therefore, we may further suppose that $c \equiv o \pmod{N_o}$

Third Step (After the assumptions $(d, N_o) = 1$, $b \equiv c \equiv o \pmod{N_o}$ are made).

We have $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} a & o \\ o & d \end{pmatrix} \pmod{N_o}$

Since $ad - bc = 1$, and $bc \equiv o \pmod{N_o}$, we have

$$ad \equiv 1 \pmod{N_o}, \quad \text{so} \quad A \equiv B \pmod{N_o} ,$$

where $B = \begin{pmatrix} a & ad-1 \\ 1-ad & d(2-ad) \end{pmatrix}$,

and so we have $A = B\,C$, for some $C \in \Gamma(N_o) \subseteq G$.

The matrix B may be written as the product:

$$B = \begin{pmatrix} 1 & 0 \\ 1-d & 1 \end{pmatrix} \begin{pmatrix} a & a-1 \\ 1-a & 2-a \end{pmatrix} \begin{pmatrix} 1 & d-1 \\ 0 & 1 \end{pmatrix}$$

Since $d \equiv 1 \pmod{N}$, $N \mid d-1$, and therefore $\begin{pmatrix} 1 & d-1 \\ 0 & 1 \end{pmatrix} \in G$ .Since (3), $\begin{pmatrix} 1 & 0 \\ 1-d & 1 \end{pmatrix} \in G$.

The middle factor can be written as

$$\begin{pmatrix} a & a-1 \\ 1-a & 2-a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & a-1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad (4)$$

Since $a \equiv 1 \pmod{N}$, $\begin{pmatrix} 1 & a-1 \\ 0 & 1 \end{pmatrix} = T^{\frac{a-1}{N} \cdot N}$,

and therefore, by the definition of the level of G, the right hand side of (4) lies in G, and hence $\begin{pmatrix} a & a-1 \\ 1-a & 2-a \end{pmatrix} \in G$.

Therefore, since B, C both lie in G, we have also $A \in G$, and this proves our claim.

2.5 The Action of a Subgroup $\hat{G}$ of $\hat{\Gamma}$ on $\mathfrak{H}^*$ - Cusps of $\hat{G}$

Let $\hat{G}$ be any subgroup of $\hat{\Gamma}$ of finite index.

The action of $\hat{\Gamma}$ on $\mathfrak{H}^*$ restricted to the subgroup $\hat{G}$ induces the action of $\hat{G}$ on $\mathfrak{H}^*$.

A similar definition to (def. I. 2.2.2) states for fundamental domains of $\hat{G}$ for $\mathfrak{H}^*$.

Definition (Def. I. 2.5.1)

Let $\hat{G}$ be any subgroup of $\hat{\Gamma}$ of finite index.

Every cusp of $\hat{\Gamma}$ fixed by an element of $\hat{G}$ is called a cusp of $\hat{G}$.

Theorem (Th. I. 2.5.2)

Let c, d, c_1, d_1 be integers, and $(c,d) = (c_1, d_1) = 1$ Then $-\frac{d}{c}$, $-\frac{d_1}{c_1}$ are equivalent cusps of $\hat{\Gamma}(n)$, if and only if,

$$(c,d) \equiv \pm (c_1, d_1) \pmod{n}$$

Proof

The rationals, $-\frac{d}{c}$, $-\frac{d_1}{c_1}$ are equivalent cusps of $\hat{\Gamma}(n)$, if and only if,

$$V\left(-\frac{d}{c}\right) = -\frac{d_1}{c_1}, \text{ for some } V \in \hat{\Gamma}(n)$$

that is, since (Th. I. 2.2.5),

$$L_1^{-1} T^k L \in \hat{\Gamma}(n) \text{ for some integer } k, \text{ where } L, L_1$$

are the inhomoneneous images of the matrices, $L = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $L_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ of $\Gamma(1)$, respectively.

Therefore $-\frac{d}{c}$, $-\frac{d_1}{c_1}$ are equivalent cusps of $\hat{\Gamma}(n)$, if and only if, there is an integer K, such that, the matrix congruence:

$$L_1 L^{-1} \equiv \pm T^K \pmod{n}$$

holds, that is,there is an integer K, so that

$$a_1 d - b_1 c \equiv \pm 1 \pmod{n}, \qquad (1)$$

$$c_1 d - d_1 c \equiv 0 \pmod{n}, \qquad (2)$$

$$-c_1 b + d_1 a \equiv \pm 1 \pmod{n}, \qquad (3)$$

and $$-a_1 b + b_1 a \equiv \pm k \pmod{n}, \qquad (4)$$

where on the right hand sides the same sign is to be taken. Note, that in the above four concruences only the (4) is depended on K.

Supposing that (1), (2) both hold, one has:

$$a_1 (d - d_1) + b_1 (c_1 - c) \equiv 0, -2 \pmod{n},$$

and $$c (d - d_1) + d (c_1 - c) \equiv 0 \pmod{n}$$

from which deduces that

$$c \equiv \pm c_1 \pmod{n}, \; d \equiv \pm d_1 \pmod{n} \qquad (5),$$

where again the right hand sides have the same sign.

Now it is easy to check, that, when the congruences (5) hold,then (1), (2) and (3) hold as well.

Thus, the above mentioned cusps are equivalent under $\hat{\Gamma}(n)$, if and only if:

$$(c, d) \equiv \pm (c_1, d_1) \pmod{n},$$

and $-a_1 b + b_1 a \equiv \pm K \pmod{n}$, for some integer K . Now, since for any integer K, we can choose the elements a, b, a_1, b_1 so that the last congruence holds, we further reduce our case to that:

$$(c, d) \equiv \pm (c_1, d_1) \pmod{n}$$

Therefore the theorem holds.

Now we denote by $\hat{\lambda}(n)$ the number of inequivalent cusps of $\hat{\Gamma}(n)$. We say that a pair of integers c, d is primitive modn, if $(c, d, n) = 1$.

From the above theorem we deduce that:

If $n > 2$, $\hat{\lambda}(n)$ is equal to the one half of the number of incongruent modn primitive pairs modn, and, if $n = 2$, $\hat{\lambda}(n)$ is just equal to this number.

Now, by counting all incongruent modn primitive pairs modn, one can prove that:

Theorem (Th. I. 2.5.3)

The number of inequivalent cusps of $\hat{\Gamma}(n)$ is given by:

$$\hat{\lambda}(n) = \frac{\hat{\mu}(n)}{n} = \begin{cases} 3 & , \text{ if } n = 2 \\ \frac{1}{2} n^2 \prod_{p|n} \left(1 - \frac{1}{p^2}\right) & , \text{ if } n > 2 \end{cases}$$

Remark (Rem. I. 2.5.4)

Using (Th. I. 2.5.2) and (Th. I. 2.5.3), we are able to determine complete systems of inequivalent cusps of $\hat{\Gamma}(n)$.

The table which follows gives some examples.

n	$\hat{\lambda}(n)$	A complete system of inequivalent cusps of $\hat{\Gamma}(n)$
2	3	$\frac{0}{1}, \frac{1}{0}, \frac{1}{1}$
3	4	$\frac{0}{1}, \frac{1}{0}, \frac{1}{1}, \frac{2}{1}$
4	6	$\frac{0}{1}, \frac{1}{0}, \frac{1}{1}, \frac{2}{1}, \frac{2}{3}, \frac{3}{1}$
5	12	$\frac{0}{1}, \frac{1}{0}, \frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{3}{1}, \frac{3}{2}, \frac{4}{1}, \frac{2}{5}, \frac{5}{2}, \frac{7}{2}, \frac{9}{2}$
6	12	$\frac{0}{1}, \frac{1}{0}, \frac{1}{1}, \frac{2}{1}, \frac{3}{1}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}, \frac{5}{1}, \frac{5}{2}, \frac{5}{3}, \frac{5}{4}$

3. MODULAR FUNCTIONS AND MODULAR FORMS

3.1 Weakly Modular Functions

Let G be any subgroup of $\Gamma(1)$ with inhomogeneous image $\hat{G}$ of finite index in the modular group $\hat{\Gamma}$, and let f be a meromorphic function on $\mathfrak{H}$, which satisfies the condition:

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^{2k} f(\tau), \qquad \text{(I. 3.1.1)}$$

$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, $\forall \tau \in \mathfrak{H}$, where k is an integer .

In this case, if we replace $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ by $-\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ the condition (I. 3.1.1) remains unchanged. Therefore, as far as (I. 3.1.1) is concerned it makes no difference whether we mark G or $\hat{G}$.

Definition (Def. I. 3.1.2)

Let G be any subgroup of $\hat{\Gamma}$, of finite index, and k be any integer. A function f is said to be a weakly modular function, of weight 2k, f or the subgroup G, if it satisfies the following two conditions:

(i) $f(\tau)$ is meromorphic on $\mathfrak{H}$, and

(ii) $f\left(\frac{a\tau + b}{c\tau + c}\right) = (c\tau + d)^{2k} f(\tau), \forall \tau \in \mathfrak{H}, \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$

In particular, if N is the least positive integer, such that the condition (ii) holds $\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(N)$, then we say that f is a weakly modular function, of weight 2k and of level N.

Theorem (Th. I. 3.1.3)

Let G be any subgroup of Γ , of finite index, and $f(\tau)$ be a meremorphic function on $\mathfrak{H}$.

Then $f(\tau)$ is a weakly modular function of weight 2k, $k \in \mathbb{Z}$, for G, if and only if, the condition

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^{2k} f(\tau),$$

holds for every generator $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of G.

In particular $f(\tau)$ is a weakly modular function of weight 2k, for $\hat{\Gamma}$,

if and only if,

$$f\ (\tau + 1) = f(\tau),$$

and $$f\ (-\tfrac{1}{\tau}) = \tau^{2k} f(\tau).$$

Proof

Let $\mathcal{M}(\mathfrak{H})$ be the set of all mereomorphic functions on $\mathfrak{H}$. For, $f \in \mathcal{M}(\mathfrak{H})$, $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, we define the function $f|_{[\sigma]_{2k}} \in \mathcal{M}(\mathfrak{H})$ by:

$$f|_{[\sigma]_{2k}}(\tau) = f\left(\frac{a\tau + b}{c\tau + d}\right)(c\tau + d)^{-2k}$$

By simple calculations, we see that G acts on $\mathcal{M}(\mathfrak{H})$, by:

$$\sigma.f = f_{|[\sigma]_{2k}}, \quad \forall \sigma \in G, \quad \forall\ f \in \mathcal{M}(\mathfrak{H})$$

Now, f is of weight 2 k, for G, if and only if,

$$\sigma.f = f \quad \forall\ \sigma \in G \qquad (1)$$

On the other hand, if (1) holds for every geneator σ of G, then it is clear that (1) holds for very element of G. This proves our claim.

In the case, where G is the whole modular group $\hat{\Gamma}$, our claim follows immediately, since $\hat{\Gamma}$ is generated by $S: \tau \longrightarrow -\frac{1}{\tau}$ and $T: \tau \longrightarrow \tau+1$ Therefore the theorem holds.

Now, for every $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$, we put

$$\nu(\gamma, \tau) = c\tau + d$$

It is easy to prove that, for every U, and V in $\Gamma(1)$ we have:

$$\nu(U\ V, \tau) = \nu(U,\ V(\tau)) \cdot \nu(V, \tau) \qquad (I.\ 3.1.4)$$

We also note, that the condition (I. 3.1.1) can be written as:

$$f\ (g(\tau)) = \nu(g, \tau)^{2k} \cdot f\ (\tau), \quad g \in G, \ \tau \in \mathfrak{H}$$

We prove now that:

Theorem (Th. I. 3.1.5)

If $f(\tau)$ is a weakly modular function of weight 2k for G, the the function

$$f|_{[\gamma^{-1}]_{2k}}(\tau) = \nu(\gamma^{-1}, \tau) \cdot f\ (\gamma^{-1}(\tau)), \qquad (1)$$

is also weakly modular of weight 2k, for $G^* = \gamma G \gamma^{-1}$.

Let g^* be in G^*, and $g^* = \mu g \mu^{-1}$, for some $g \in G$.

We have

$$f|_{[\mu^{-1}]_{2k}}(g^*(\tau)) = \vartheta(\mu^{-1}, g^*(\tau))^{-2k} \cdot f(\mu^{-1} g^*(\tau))$$
$$= \vartheta(\mu^{-1}, \mu g \mu^{-1}(\tau))^{-2k} \cdot f(g\mu^{-1}(\tau))$$
$$= \vartheta(\mu^{-1}, \mu g \mu^{-1}(\tau))^{-2k} \vartheta(g, \mu^{-1}(\tau))^{2k} \cdot f(\mu^{-1}(\tau))$$
$$= \vartheta(\mu^{-1}, \mu g \mu^{-1}(\tau))^{-2k} \cdot \vartheta(g, \mu^{-1}(\tau))^{2k} \cdot \vartheta(\mu^{-1}, \tau)^{2k} \cdot f|_{[\mu^{-1}]_{2k}}(\tau)$$
$$= \left[\vartheta(\mu^{-1}, \mu g \mu^{-1}(\tau)) \cdot \vartheta(g, \mu^{-1}(\tau))^{-1} \cdot \vartheta(\mu^{-1}, \tau)^{-1}\right]^{-2k} \cdot f|_{[\mu^{-1}]_{2k}}(\tau)$$

Because of (I. 3.1.4), $\vartheta(g, \mu^{-1}(\tau))\,\vartheta(\mu^{-1}, \tau) = \vartheta(g\mu^{-1}, \tau)$ and also $\vartheta(\mu^{-1}, \mu g \mu^{-1}(\tau)) = \vartheta(g\mu^{-1}, \tau) \cdot \vartheta(\mu g \mu^{-1}, \tau)^{-1}$

Therefore:

$$f|_{[\mu^{-1}]_{2k}}(g^*(\tau)) = \left[\vartheta(g\mu^{-1}, \tau) \cdot \vartheta(\mu g \mu^{-1}, \tau)^{-1} \cdot \vartheta(g\mu^{-1}, \tau)^{-1}\right]^{-2k} \cdot f|_{[\mu^{-1}]_{2k}}(\tau)$$
$$= \vartheta(\mu g \mu^{-1}, \tau)^{2k} \cdot f|_{[\mu^{-1}]_{2k}}(\tau)$$
$$= \vartheta(g^*, \tau)^{2k} \cdot f|_{[\mu^{-1}]_{2k}}(\tau)$$

hence the theorem holds, since the condition (i) of (Def. I.3.1.2) is easily verified .

We now consider the behaviour of a weakly modular function f, of weight 2k, for G, at $i\infty$, and a rational cusp $-\frac{d}{c}$, $c \neq 0$, $(c, d) = 1$, if one exists.

So, let lev (g) = N

For any positive number a, we set

$$\mathfrak{H}_a = \left\{ \tau \in \mathfrak{H} \ : \ \mathrm{jm}\ (\tau) > a \right\}$$

Then the function $h(\tau) = e^{2\pi i \tau / N}$ maps $\mathfrak{H}_a$ onto the punctured disk:

$$D = \left\{ q \in \mathbb{C} \ : \ 0 < |q| < e^{-2\pi a / N} \right\}$$

Since lev (G) = N, the function f is periodic with period N.

On the other hand, for $\tau \in \mathfrak{H}_a$, $h^{-1}(h(\tau)) = \left\{ \tau + kN \ : \ k \in \mathbb{Z} \right\}$

We note that $f(\tau + kN) = f(\tau)$, $\quad k \in \mathbb{Z}$.

Therefore, setting $q = e^{2\pi i \tau}$, the function of $f(\tau)$ depends only on $q^{1/N}$, so induces a meromorphic function

$$\Phi : D \longrightarrow \mathbb{C}$$

such that $f(\tau) = \Phi(q^{1/N})$.

We make, now, the following definitions:

Definitions (Def. I. 3.1.6)

If Φ extends to a meromorphic function at the origin q = o, we say that $f(\tau)$ is meromorphic at infinity.

In this case Φ has a Laurent expansion in a neighbourhood of the origin of the form:

$$\Phi(q^{1/N}) = \sum_{n=-m}^{\infty} c_n q^{n/N} ,$$

where $-m \in \mathbb{Z} \setminus \{0\}$.

This induces a Fourier expansion for $f(\tau)$,

$$f(\tau) = \sum_{n=-m}^{\infty} c_n e^{2\pi i \tau n / N}$$

which is valid for a sufficiently large jm (τ), and is called

Fourier expansion for $f(\tau)$ at $i\infty$.

In particular, if $f(\tau)$ is meromorphic at $i\infty$ then, $-m \geq 0$, that is:

$$f(\tau) = \sum_{n=0}^{\infty} c_n e^{2\pi i \tau n / N}$$

In this case we write $f(i\infty) = C_0$, and the constant C_0 is called

the value of $f(\tau)$ at $i\infty$.

If $f(\tau)$ is strictly meromorphic at infinity then $-m < 0$.

In this case we say that $f(\tau)$ has a pole of order m at infinity.

Now the behaviour of $f(\tau)$ at a rational cusp of G, if one exists, is handled by reducing the problem to the case at infinity.

We proceed as follows:

Let $-\frac{d}{c}$, $c \neq 0$, $(c, d) = 1$, be a rational cusp of G, and let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$, such that $\gamma(-\frac{d}{c}) = i\infty$.

Now setting

$$g(\tau) = f\big|[\gamma^{-1}]_{2K}(\tau) = (-c\tau + a)^{-2K} f(\gamma^{-1}(\tau)) \qquad (I.3.1.7)$$

we note that:

By (Th. I. 3.1.5), $g(\tau)$ is also a weakly modular function of weight 2k, for $G^* = \gamma G \gamma^{-1}$. We also note that $\text{lev}(G^*) = \text{lev}(G)$ and $\gamma^{-1}(i\infty) = -\frac{d}{c}$. Finally, the behaviour of $g(\tau)$ at $i\infty$, does not depend on the choice of γ, since, by (Th. I.2.2.5 (i)), the cusp $-\frac{d}{c}$ determines the transformation γ up to a factor of T^n with an arbitrary interger n.

Therefore the following definition makes sense:

Definition (Def. I. 3.1.8)

Keeping fixed the above notation, we say that the behaviour of $f(\tau)$ at the rational cusp $-\frac{d}{c}$, is that of $g(\tau)$ at $i\infty$.

3.2 Modular Functions

Definition (Def. I. 3.2.1)

Let G be any subgroup of $\hat{\Gamma}$ of finite index, and K be any integer.

A function f is defined to be a modular function of weight 2k, for the subgroup G, if it satisfies the following conditions:

(i) $f(\tau)$ is a weakly modular function of weight 2k, for the subgroup G, and

(ii) $f(\tau)$ is meromorphic at $i\infty$, and also at all rational

cusps of G, if one exists.

It is easily seen that:

Remark (Rem I. 3.2.2)

If f (τ) is a weakly modular function of weight 2k for the whole modular group, then the behaviour of f (τ) at a rational cusp follows that at infinity.

3.3 Modular Forms

Definition (Def. I. 3.3.1)

Let G be any subgroup of $\hat{\Gamma}$, of finite index, and k be any integer. A modular function, of weight 2k, for G, which is holomorphic on $\mathfrak{H}$ and also at all the cusps of G is said to be a modular form, of weight 2k, for G.

3.4 Cusp Forms

Definition (Def. I. 3.4.1)

Let G be any subgroup of $\hat{\Gamma}$, of finite index, and k be any integer. A modular form, of weight 2k, for G, which vanishes at all the cusps of G, is called a cusp form, of weight 2k, for G.

3.5 The Vector Space of Modular Forms

In this paragraph, we state, without proof, some important theorems.

We denote by $D_{\hat{\Gamma}}$, the fundamental domain of $\hat{\Gamma}$ for $\mathfrak{H}^*$, which we have defined in the (Th. I. 2.2.3). Now, let f be any modular function of weight 2k for $\hat{\Gamma}$, and τ be any point in $D_{\hat{\Gamma}}$. If $\tau \in D_{\hat{\Gamma}} \setminus \{i\infty\}$, and there is an integer n such that $f(z) = (z - \tau)^n h(z)$, where $h(z)$ is holomorphic and non-zero at τ, then this is called the order of f at τ, and is denoted by $U_\tau(f)$.

If $\tau = i\infty$, we define the order of f at $i\infty$, and denote by $U_{i\infty}(f)$, the order of the function $\Phi(q^{1/N})$ at $q = 0$, where Φ is the function defined § 3.1 .

Theorem (Th. I. 3.5.1) (See Serre [38] p.p. 85, Th. 3)

If f is a non-zero modular function, of weight 2k for $\hat{\Gamma}$, then the following formula holds:

$$U_{i\infty}(f) + \frac{1}{2} U_i(f) + \frac{1}{3} U_\rho(f) + \sum_{\substack{\tau \in D_{\hat{\Gamma}} \\ \tau \neq i\infty, i, \rho}} U_\tau(f) = \frac{k}{6}$$

where $\rho = e^{2\pi i/3}$.

Quoting from Gunning ([21] , p.p. 25-26), and Serre ([38] , Chapter VII, § 3, Theorem 4), we state a general theorem of the vector space of modular forms.

Theorem (Th. I. 3.5.2)

Let G be any subgroup of $\hat{\Gamma}$, of finite index. Denote by $M_k(G)$ (resp. $M_k^0(G)$) the $\mathbb{C}$-vector space of modular forms of weight 2k for G (resp. of cusp forms of weight 2k for G, and $\delta_k(G)$ (resp. $\delta_k^0(G)$) its dimension.

We have:

$$\delta_k(G) = \begin{cases} 0 & , \text{if } k \leq 1, k \neq 0. \\ 1 & , \text{if } k = 0. \\ (2k-1)(g-1) + \sigma k + \sum_i \left[k \left(1 - \frac{1}{e_i}\right) \right] & , \text{if } k > 1. \end{cases}$$

where g is the genus of the Riemann surface of $\mathfrak{H}^*/G$, σ is the number of cusps of G, and the sum runs through the elliptic fixed points of G of periods e_i.

In particular:

(i) For the full modular group $\hat{\Gamma}$:

$$\delta_k(\hat{\Gamma}) = \begin{cases} [k/6] & , \text{if } k \equiv 1 \pmod 6 \\ [k/6] + 1 & , \text{if } k \not\equiv 1 \pmod 6 \end{cases}$$

$$\delta_k^0(\hat{\Gamma}) = \delta_{k-6}(\hat{\Gamma})$$

For k = 0, 2, 3, 4, 5, $M_k(\hat{\Gamma})$ is of dimension 1 with a basis 1, G_2, G_3, G_4, G_5 respectively. Also $\delta_k^0(\hat{\Gamma}) = 0$ for k = 0, 2, 3, 4, 5.

(ii) For the principal congruence subgroup $\hat{\Gamma}(2)$:

$$\delta_k(\hat{\Gamma}(2)) = k + 1$$

(iii) For the principal congruence subgroup $\hat{\Gamma}(n)$, $n \geq 3$:

$$\delta_k(\hat{\Gamma}(n)) = \frac{(2k-1)n + 6}{24} n^2 \prod_{p|n} \left(1 - \frac{1}{p^2}\right).$$

4. Examples of Modular Functions and Forms

4.1 The Basic Functions $g_2(\tau)$, $g_3(\tau)$

Since, for $k \geq 2$, the Eisenstein series:

$$G_k(\tau) = \sum_{(c,d)\neq(0,0)} \frac{1}{(c\tau + d)^{2k}}, \quad k \geq 2$$

is absolutely convergent, it is easy to see that it gives a modular form of weight 2k, for $\hat{\Gamma}$. Furthermore,

$$G_k(i\infty) = \sum_{n\neq 0} \frac{1}{n^{2k}} = 2\zeta(2k),$$

where ζ denotes the Riemann zeta function.

Therefore, $G_k(\tau)$ is not a cusp form.

Consequently the basic functions

$$g_2(\tau) = 60\, G_2(\tau)$$

$$g_3(\tau) = 140\, G_3(\tau)$$

are modular forms of weight 4,6 respectively, for $\hat{\Gamma}$.

These are not cusp forms, and in fact

$$g_2(i\infty) = 2\zeta(4) = \frac{4}{3}\pi^4,$$

$$g_3(i\infty) = 2\zeta(6) = \frac{8}{27}\pi^6 \qquad \text{(I. 4.1.1)}$$

The Fourier expansion of these functions are given by

$$g_2(\tau) = \frac{4\pi^4}{3}\left\{1 + 240 \sum_{k=1}^{\infty} \sigma_3(k)\, q^k\right\},$$

$$g_3(\tau) = \frac{8\pi^6}{27}\left\{1 - 504 \sum_{k=1}^{\infty} \sigma_5(k)\, q^k\right\} \qquad \text{(I. 4.1.2)}$$

where $q = e^{2\pi i\tau}$, $\sigma_\alpha(k) = \sum_{d|k} d^\alpha$ (see Serre [38], p.p. 93)

4.2 The Discriminant $\Delta(\tau)$

Using the above facts, for the basic functions $g_2(\tau)$, $g_3(\tau)$, we deduce that the discriminant:

$$\Delta(\tau) = g_2^3(\tau) - 27\, g_3^2(\tau)$$

is a modular form of weight 12, for $\hat{\Gamma}$. Furthermore, from (I. 4.1.1) we have $\Delta(i\infty) = 0$. Thus $\Delta(\tau)$ is a cusp form of weight 12, for $\hat{\Gamma}$.

By (Th. I. 3.5.2 (i)), $\delta_6^0(\hat{\Gamma}) = \delta_0(\hat{\Gamma}) = 1$, and therefore <u>the discriminant $\Delta(\tau)$ is the only cusp form, up to scalar multiples, of weight 12, for $\hat{\Gamma}$</u>.

By (I. 4.1.2), the Fourier expansion of $\Delta(\tau)$ is given by

$$\Delta(\tau) = (2\pi)^{12}\,(q - 24q^2 + 252q^3 - 1472q^4 + \cdots) \qquad \text{(I. 4.2.1)}$$

Furthermore, we state the Jacobi formula for Δ,

$$\Delta(\tau) = (2\pi)^{12}\, q \prod_{n=1}^{\infty} (1 - q^n)^{24}, \qquad \text{(I. 4.2.2)}$$

The proof may be sketched as follows:

Set $h(\tau) = (2\pi)^{12} q \prod_{n=1}^{\infty} (1 - q^n)^{24}$, and show that

$$h(\tau + 1) = h(\tau), \quad h\left(-\frac{1}{\tau}\right) = \tau^{12} h(\tau)$$

This proves that $h(\tau)$ is a cusp form of weight 12, for $\hat{\Gamma}$. Therefore $\Delta(\tau) = c\, h(\tau)$ for some constant $c \in \mathbb{C}$. Since (I. 4.2.1), we have:

$$1 - 24q + \cdots = c \prod_{n=1}^{\infty} (1 - q^n)^{24}$$

which gives $c = 1$ (for $q = 0$). Thus (I. 4.2.2) holds.

Finally, from (I. 4.2.2), we deduce that:

$$\Delta(\tau) \neq 0 \qquad \forall \tau \in \mathfrak{H} \qquad \text{(I. 4.2.3)}$$

4.3 The Absolute Invariant $j(\tau)$

The absolute invariant $j(\tau)$ is given by

$$j(\tau) = 1728 \cdot \frac{g_2^3(\tau)}{\Delta(\tau)}$$

Using the facts about $g_2(\tau)$, $\Delta(\tau)$ of the previous examples, we decude that $j(\tau)$ is holomorphic on $\mathfrak{H}$. Writing I for any power series in q with integer coefficients, we deduce from (I. 4.1.2) that:

$$g_2^3(\tau) = \frac{64\pi^{12}}{27} \quad (1 + 720q + I),$$

and $$\Delta(\tau) = 1728 \quad \frac{64\pi^{12}}{27} q \quad (1 - 24q + I)$$

Therefore $$j(\tau) = \frac{1 + 720q + I}{q\,(1 - 24q + I)}$$

and thus: $$j(\tau) = \frac{1}{q} \quad (1 + 720\,q + I)\,(1 + 24q + I)$$

Hence: $$j(\tau) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c_n\, q^n, \qquad \text{(I. 4.3.1)}$$

where c_n are integers.

The expansion (I. 4.3.1) begins with

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots$$

So the function $j(\tau)$ has a simple pole at $i\infty$ with residue 1.

Now, since $g_2^3(\tau)$, and $\Delta(\tau)$ are modular functions of the same weight, for $\hat{\Gamma}$, we have:

$j(\tau)$ is a modular function of weight 0, for $\hat{\Gamma}$.

We state, now, some important properties of the absolute invariant j.

Theorem (Th. I. 4.3.2)

The map $j: \mathcal{H}^*/\hat{\Gamma} \longrightarrow \bar{\mathbb{C}}$ is a bijection, or equivalently, since the (Rem. I. 2.2.4), the map $j: D_{\hat{\Gamma}} \longrightarrow \bar{\mathbb{C}}$ is a bijection.

In particular:

$j(i\infty) = \infty$, $j(\tau)$ has a triple zero at $\tau = \rho = e^{2\pi i/3}$, and $j(\tau) - 1728$ has a double zero at $\tau = i$.

Proof

Let c be any complex number.

Set $f(\tau) = j(\tau) - c$.

The function $f(\tau)$ is modular of weight 0 for $\hat{\Gamma}$, holomorphic on $\mathcal{H}$, and has a simple pole at $i\infty$.

By the (Th. I. 3.5.1), we have

$$\frac{1}{2} U_i(f) + \frac{1}{3} U_\rho(f) + \sum_{\substack{\tau \in D_{\hat{\Gamma}} \\ \tau \neq i\infty, i, \rho}} U_\tau(f) = 1 \qquad (1)$$

and since $f(\tau)$ is holomorphic on $\mathcal{H}$, the terms on the left are all ≥ 0.

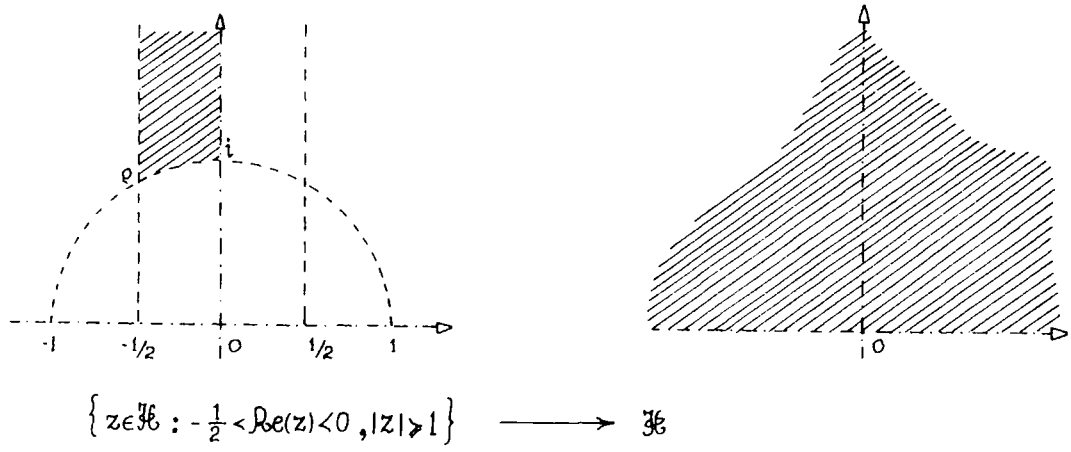
Therefore the sum contains only one term, $U_\tau(f)$, and (1) holds, if and only if,

$$\left(U_i(f),\ U_\rho(f),\ U_\tau(f)\right) = (0,\ 0,\ 1) \text{ or } (2,\ 0.\ 0) \text{ or } (0,\ 3,\ 0) \qquad (2)$$

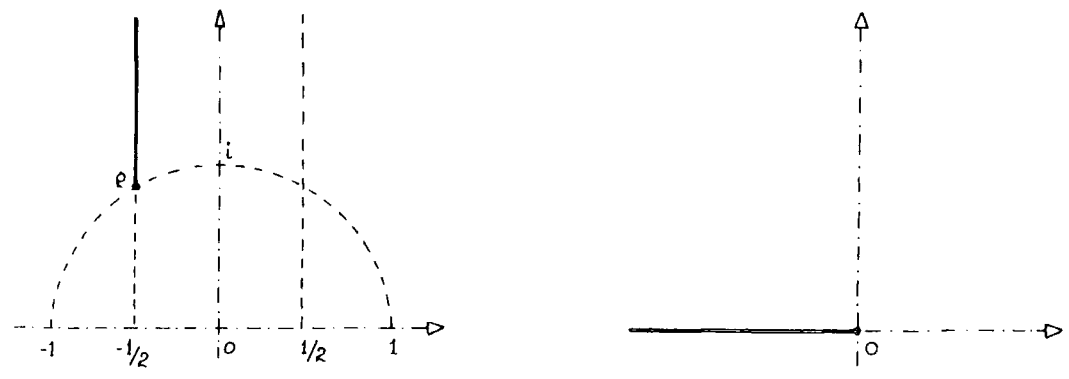
Thus, in every case, there is a unique $\tau \in D_{\hat{f}} \setminus \{i\infty\}$ such that $j(\tau) = c$. Therefore adding the case $j(i\infty) = \infty$, we proved that the map $j : D_{\hat{f}} \longrightarrow \bar{\mathbb{C}}$ is a bijection.

Also, since (2), the multiplicity of $j(\tau) = 1728$ is 2 at $\tau = i$, and the multiplicity of $j(\tau) = 0$ is 3 at $\tau = \rho$. In all other cases the multiplicity is 1.

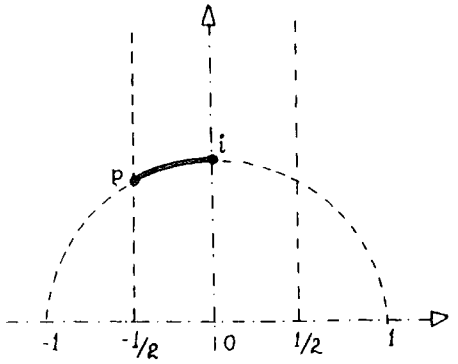
The following figures illustrate how $D_{\hat{f}}$ is mapped by j onto the complex plane.



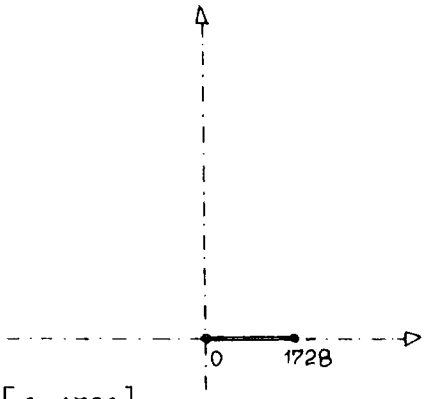
$$\left\{z \in \mathcal{H} : -\tfrac{1}{2} < Re(z) < 0,\ |z| > 1\right\} \longrightarrow \mathcal{H}$$



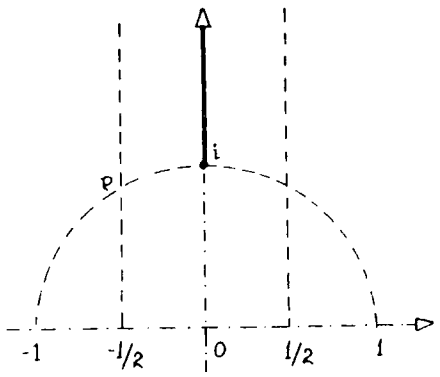
$$\left\{z \in \mathcal{H} :\ Re(z) = -\tfrac{1}{2},\ |z| > 1\right\} \longrightarrow (-\infty, 0]$$



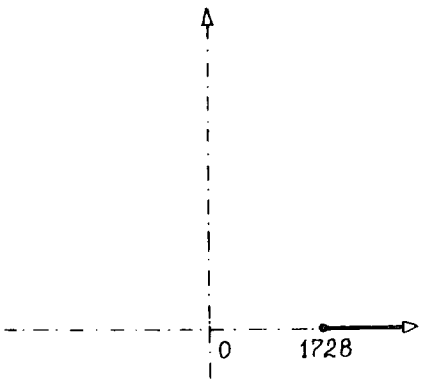
$\{z\in\mathcal{H} : \frac{\pi}{2} \leq \arg z < \frac{2\pi}{3} \ , \ |z|=1\}$ $\longrightarrow$



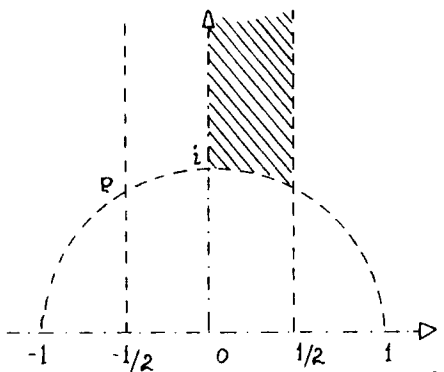
$[0, 1728]$



$\{z\in\mathcal{H} : \mathcal{R}e(z)=0 \ , \ \mathcal{I}m(z)\geq 1\}$ $\longrightarrow$

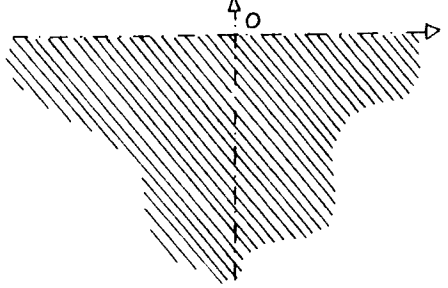


$[1728, +\infty]$



$\{z\in\mathcal{H} : 0 < \mathcal{R}e(z) < \frac{1}{2} \ , \ |z|>1\}$ $\longrightarrow$

$\{z\in\mathbb{C} : \mathcal{I}m(z)<0\}$



Theorem (Th. I. 4.3.3)

(i) Every modular function of weight 0, for $\hat{\Gamma}$, can be expressed as a rational function of j, and conversely.

(ii) In particular, if $f(\tau)$ is a modular function of weight 0 for $\hat{\Gamma}$, holomorphic on $\mathfrak{H}$, with Fourier expansion:

$$f(\tau) = \sum_{n=-m}^{\infty} c_n q^n \quad , \quad q = e^{2\pi i \tau} \qquad (1)$$

then f can be expressed as a polynomial in j with coefficients in the $\mathbb{Z}$-module generated by the coefficients c_i, $(i \geq -m)$, occured in (1).

Proof

We are interested in showing (ii), since the first part of the theorem is well-known (see Serre [38], p.p. 89, Pr. 6). Note, that the j function is also holomorphic on $\mathfrak{H}$ with Fourier expansion:

$$j(\tau) = \frac{1}{q} + \sum_{n=0}^{\infty} a_n q^n \quad , \quad \text{where} \quad a_i \in \mathbb{Z} \quad \forall\, i = 0, 1, 2, \ldots$$

Thus the new function $f - c_{-m} j^m$ is again holomorphic on $\mathfrak{H}$, and has a Fourier expansion.

$$(f - c_{-m} j^m)(\tau) = \sum_{n=-m+1}^{\infty} b_n \cdot q^n$$

Now we form the new function $f - c_{-m} j^m - b_{-m+1} j^{m-1}$, which is also holomorphic on $\mathfrak{H}$.

Continuing this process we find a function

$$f - c_{-m} j^m - b_{-m+1} j^{m-1} - \ldots - \kappa_1 j - \lambda_0 \qquad (2)$$

which is modular of weight 0 for $\hat{\Gamma}$, holomorphic at $i\infty$ and indeed vanishes there. So, this is a cusp form of weight 0 for $\hat{\Gamma}$, and since $\mathcal{O}_0^{\infty}(\hat{\Gamma}) = 0$ (Th. I. 5.3.2 (i)), the function (2) is identically zero, and by construction all coefficients occurred in (2) lie in the $\mathbb{Z}$-module generated by $C_i^{'s}$.

4.4 The 8th Power of the Dedekind eta Function

The Dedekind eta function is defined by

$$\eta_0(\tau) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n), \quad q = e^{2\pi i \tau}$$

Since $|q| < 1$, the infinite product converges absolutely and is

non-zero. Furthermore, since the convergence is uniform on compact subsets of $\mathcal{H}$, $\eta(\tau)$ is holomorphic on $\mathcal{H}$. Also note that $\eta(\tau)$ is holomorphic at infinity, and indeed $\eta(i\infty) = 0$. It is clear that $\eta(\tau + 1) = e^{2\pi i/24}\eta(\tau)$. It is also true that $\eta(-\frac{1}{\tau}) = \sqrt{-i\tau}\ \eta(\tau)$ (e.g. see Seigel's proof [41]). Therefore, the action of $\hat{\Gamma}$ on η is given by:

$$\eta(\tau + 1) = e^{2\pi i/24}\eta(\tau),\ \eta(-\frac{1}{\tau}) = \sqrt{-i\tau}\ \eta(\tau) \qquad \text{(I. 4.4.1)}$$

where the square root takes positive values on the positive real axis. Thus, we can easily deduce that:

<u>The function $\eta^{24}(\tau)$ is a cusp form of weight 12, for $\hat{\Gamma}$.</u>

Clearly, in view of (I. 4.2.2)

$$\Delta(\tau) = (2\pi)^{12}\eta^{24}(\tau) \qquad \text{(I. 4.4.2)}$$

and that proves again our previous statement for $\eta^{24}(\tau)$.

Also, in view of (I. 4.4.2), $\eta(\tau) \neq 0 \quad \forall \tau \in \mathcal{H}$.

For the 8th power of η, we have :

$$\eta^8(\tau + 1) = e^{2\pi i/3}\eta^8(\tau),\quad \eta^8(-\frac{1}{\tau}) = \tau^4 \cdot \eta^8(\tau)$$

We now look at the function $\eta^8(\tau)$ under the action of $\hat{\Gamma}(3)$.

We know that $\Gamma(3)$ is generated by the matrices:

$$T^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix},\quad (ST)^{-1}\ T^3\ (ST) = \begin{pmatrix} 4 & 3 \\ -3 & -2 \end{pmatrix},\quad (ST)^{-2}\ T^3\ (ST)^2 = \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix}$$

One easily calculates that

$$\eta^8(\tau + 3) = \eta^8(\tau)$$

$$\eta^8\left(\frac{4\tau + 3}{-3\tau - 2}\right) = (3\tau + 2)^4 \cdot \eta^8(\tau)$$

$$\eta^8\left(\frac{\tau}{-3\tau + 1}\right) = (3\tau - 1)^4\ \eta^8(\tau)$$

And so, by (Th. I. 3.1.3) $\eta^8(\tau)$ is a weakly modular function of weight 4, for $\hat{\Gamma}(3)$. By (Rem I. 2.5.4), $\{i\infty, 0, 1, 2\}$ is a complete system of inequivalent cusps of $\hat{\Gamma}(3)$.

Clearly, $\eta^8(\tau)$ is holomorphic on $\mathcal{H}$.

Also, from (I. 4.4.2) and (I. 4.2.1), we have:

$$\eta^8(\tau) = (2\pi)^{-4}\Delta(\tau)^{1/3} = (q - 24q^2 + 252q^3 - 1472q^4 + \cdots)^{1/3} \qquad \text{(I. 4.4.3)}$$

and so, $\eta^8(\tau)$ is holomorphic at infinity and vanishes there.

Now let $-\frac{d}{c}$ be a rational cusp of $\hat{\Gamma}(3)$, and let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$ such that $\gamma(-\frac{d}{c}) = i\infty$.

Now in view of the (Def. I. 3.1.8), we have:

$$\eta^8\big|_{[\gamma^{-1}]_4}(\tau) = (-c\tau + a)^{-4}\,\eta^8\left(\frac{d\tau - b}{-c\tau + a}\right)$$

and in view of (I. 4.4.3),

$$\eta^8\big|_{[\gamma^{-1}]_4}(\tau) = (2\pi)^{-4}\left[\Delta(d\tau - b)\right]^{1/3}$$

and now, it is clear, from (I. 4.4.3), that $\eta^8|_{[\gamma^{-1}]_4}(\tau)$ is holomorphic at $i\infty$ and vanishes there. So, $\eta^8(\tau)$ is holomorphic at all cusps and vanishes there.

Therefore, by (Th. I. 3.5.2), the function $\eta^8(\tau)$ is the only cusp form, up to scalar multiples, of weight 4, for $\hat{\Gamma}(3)$. (I. 4.4.4)

4.5 The Weber Functions γ_2, γ_3.

Definition (Def. I. 4.5.1)

We define the Weber functions γ_2, γ_3 by,

$$\gamma_2(\tau) = \frac{3}{4\pi^4} \cdot \frac{g_2(\tau)}{\eta^8(\tau)}, \quad \gamma_3(\tau) = \left(\frac{3}{2\pi^2}\right)^3 \cdot \frac{g_3(\tau)}{\eta^{12}(\tau)} \qquad \text{(I. 4.5.1)}$$

From (I. 4.4.2), we deduce that:

$$\gamma_2^3(\tau) = j(\tau), \quad \text{and} \quad \gamma_3^2(\tau) = j(\tau) - 1728 \qquad \text{(I. 4.5.2)}$$

Since the functions $g_2(\tau)$, $g_3(\tau)$, $\eta(\tau)$ are holomorphic on $\mathcal{H}$ and $\eta(\tau) \neq 0\ \forall \tau \in \mathcal{H}$, we have $\gamma_2(\tau)$, $\gamma_3(\tau)$ are both holomorphic on $\mathcal{H}$.

Since $j(\tau)$ has a triple zero at $\tau = e^{2\pi i/3}$, the function $\gamma_2(\tau)$ has a simple zero at $\tau = e^{2\pi i/3}$. Also, since $j(\tau) - 1728$ has a double zero at $\tau = i$, the function $\gamma_3(\tau)$ has a simple zero at $\tau = i$.

Since the basic functions $g_2(\tau)$, $g_3(\tau)$ are modular forms of weight 4, 6 respectively, for $\hat{\Gamma}$, the action of $\hat{\Gamma}$ on them is given by:

$$g_2(\tau + 1) = g_2(\tau), \quad g_2\left(-\frac{1}{\tau}\right) = \tau^4 g_2(\tau)$$
$$g_3(\tau + 1) = g_3(\tau), \quad g_3\left(-\frac{1}{\tau}\right) = \tau^6 g_3(\tau) \qquad \text{(I. 4.5.3)}$$

Therefore the action of $\hat{\Gamma}$ on the functions γ_2, γ_3 can be easily deduced from (I. 4.5.3) and (I. 4.4.1), and is given by the following formulae:

$$\gamma_2(\tau + 1) = e^{4\pi i/3}\,\gamma_2(\tau) \quad , \quad \gamma_2\left(-\frac{1}{\tau}\right) = \gamma_2(\tau) \qquad \text{(I. 4.5.4)}$$

$$\gamma_3(\tau + 1) = -\gamma_3(\tau) \quad , \quad \gamma_3\left(-\frac{1}{\tau}\right) = -\gamma_3(\tau) \qquad \text{(I. 4.5.5)}$$

Starting from (I. 4.5.4), and following the same process as in § 4.4, one proves, by simple calculations, that the function $\gamma_2(\tau)$ is invariant under $\hat{\Gamma}(3)$.

Again, $\Gamma(2)$ is generated by the matrices

$$T^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad S\,T^2\,S = \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix} \quad , \text{ and from}$$

(I. 4.5.5), we can easily deduce, that the function $\gamma_3(\tau)$ is invariant under $\hat{\Gamma}(2)$.

So far, we have proved that $\gamma_2(\tau)$, $\gamma_3(\tau)$ are weakly modular functions of weight 0, for $\hat{\Gamma}(3)$, $\hat{\Gamma}(2)$ respectively.

Finally, we see from (I. 4.5.2), that the functions $\gamma_2(\tau)$, $\gamma_3(\tau)$ are both meromorphic at infinity.

Now let $-\frac{d}{c}$, $c \neq 0$, $(c, d) = 1$ be any rational cusp of $\hat{\Gamma}(3)$ (resp. $\hat{\Gamma}(2)$) and let

$$\rho = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \qquad \text{is such that}$$

$$\rho\left(-\frac{d}{c}\right) = i\infty \quad .$$

In view of the (Def. I. 3.1.8) we have

$$\gamma_2|_{[\rho^{-1}]_0}(\tau) = \gamma_2\left(\rho^{-1}(\tau)\right)$$

$$\left(\text{resp. } \gamma_3|_{[\rho^{-1}]_0}(\tau) = \gamma_3\left(\rho^{-1}(\tau)\right)\right)$$

and so we deduce from (I. 4.5.4) (resp. (I. 4.5.5)), that

$$\gamma_2|_{[\rho^{-1}]_0}(\tau) = \rho\,\gamma_2(\tau)$$

$$\left(\text{resp. } \gamma_3|_{[\rho^{-1}]_0}(\tau) = (\pm 1)\,\gamma_3(\tau)\right)$$

Therefore, the function $\gamma_2(\tau)$ (resp. $\gamma_3(\tau)$) is meromorphic at all rational cusps of $\hat{\Gamma}(3)$ (resp. $\hat{\Gamma}(2)$).

So we have proved that:

Theorem (Th. I. 4.5.6)

The Weber functions $\gamma_2(\tau)$, $\gamma_3(\tau)$ are modular functions of weight 0, for the subgroups $\hat{\Gamma}(3)$, $\hat{\Gamma}(2)$ respectively. Also, they are both holomorphic on $\mathfrak{H}$.

4.6 The Weber Functions f, f_1, f_2.

Definition (Def. I. 4.6.1) (See Weber [48], § 25, p.p. 86)

We define the Weber functions f, f_1, f_2 by

$$f(\tau) = q^{-1/48} \prod_{n=1}^{\infty} (1 + q^{n-\frac{1}{2}}) \qquad \text{(I. 4.6.1)}$$

$$f_1(\tau) = q^{-1/48} \prod_{n=1}^{\infty} (1 - q^{n-\frac{1}{2}})$$

$$f_2(\tau) = \sqrt{2}\, q^{1/24} \prod_{n=1}^{\infty} (1 + q^{n})$$

where $q = e^{2\pi i \tau}$.

Hence we may express these functions in terms of the Dede kind eta function η as follows:

$$f(\tau) = e^{-\pi i/24} \cdot \frac{\eta(\frac{\tau+1}{2})}{\eta(\tau)} \qquad \text{(I. 4.6.2)}$$

$$f_1(\tau) = \frac{\eta(\frac{\tau}{2})}{\eta(\tau)}$$

$$f_2(\tau) = \sqrt{2}\, \frac{\eta(2\tau)}{\eta(\tau)}$$

Since $\eta(\tau+1) = e^{2\pi i/24}\, \eta(\tau)$, and $\eta(-\frac{1}{\tau}) = \sqrt{-i\tau}\, \eta(\tau)$ (I. 4.4.1) we can easily deduce, that the action of the modular group $\hat{\Gamma}$ on the functions f, f_1, f_2 is given as follows:

$$\begin{aligned} f(\tau+1) &= e^{-\pi i/24} f_1(\tau), \quad f(-\tfrac{1}{\tau}) = f(\tau) \\ f_1(\tau+1) &= e^{-\pi i/24} f(\tau), \quad f_1(-\tfrac{1}{\tau}) = f_2(\tau) \qquad \text{(I. 4.6.3)} \\ f_2(\tau+1) &= e^{\pi i/12} f_2(\tau), \quad f_2(-\tfrac{1}{\tau}) = f_1(\tau) \end{aligned}$$

Lemma (Lem. I. 4.6.4)

$$f_1^8(\tau) + f_2^8(\tau) = f^8(\tau) \qquad \text{(I. 4.6.5)}$$

$$f^8(\tau) f_1^8(\tau) + f^8(\tau) f_2^8(\tau) - f_1^8(\tau) f_2^8(\tau) = \gamma_2(\tau) \qquad \text{(I. 4.6.6)}$$

$$f(\tau) f_1(\tau) f_2(\tau) = \sqrt{2} \qquad \text{(I. 4.6.7)}$$

Proof of the Lemma

The proof of (I. 4.6.7) easily follows from (I. 4.6.1).

Proof of (I. 4.6.5)

Put $F(\tau) = f_1^8(\tau) + f_2^8(\tau) - f^8(\tau)$

Using the action of $\hat{\Gamma}$ on the Weber functions, from (I. 4.6.3), we can easily see that:

$$F(\tau+1) = e^{2\pi i/3} F(\tau), \quad F\left(-\frac{1}{\tau}\right) = F(\tau)$$

Set $\tilde{F}(\tau) = F(\tau)\,\eta^{16}(\tau)$.

From (I. 4.4.1) we have :

$$\eta^{16}(\tau+1) = e^{4\pi i/3}\,\eta^{16}(\tau), \quad \eta^{16}\left(-\frac{1}{\tau}\right) = \tau^8\,\eta^{16}(\tau)$$

Thus:

$$\begin{aligned}\tilde{F}(\tau+1) &= F(\tau+1)\,\eta^{16}(\tau+1)\\ &= e^{2\pi i/3} F(\tau)\, e^{4\pi i/3}\,\eta^{16}(\tau)\\ &= F(\tau)\,\eta^{16}(\tau)\\ &= \tilde{F}(\tau)\end{aligned}$$

Also:

$$\begin{aligned}\tilde{F}\left(-\frac{1}{\tau}\right) &= F\left(-\frac{1}{\tau}\right)\,\eta^{16}\left(-\frac{1}{\tau}\right)\\ &= F(\tau)\,\tau^8\,\eta^{16}(\tau)\\ &= \tau^8\tilde{F}(\tau)\end{aligned}$$

So $\tilde{F}(\tau)$ is a weakly modular function of weight 8 for the full modular group $\hat{\Gamma}$. From (I. 4.6.2), and since $\eta^8(\tau)$ is holomorphic on $\mathcal{H}\cup\{i\infty\}$, and also $\eta^8(i\infty) = 0$, we have that $\tilde{F}(\tau)$ is a cusp form of weight 8 for $\hat{\Gamma}$. By (Th. I. 3.5.2 (i)), the vector space of cusp forms of weight 8, for $\hat{\Gamma}$, is actually the zero space. Hence $\tilde{F}(\tau) = 0$, that is $F(\tau) = 0$, and so (I. 4.6.5) holds.

Proof of (I. 4.6.6)

Put $$W(\tau) = f^8(\tau)\, f_1^8(\tau) + f^8(\tau)\, f_2^8(\tau) - f_1^8(\tau)\, f_2^8(\tau) - \gamma_2(\tau)$$

Again, we find that:

$$W(\tau+1) = e^{4\pi i/3} W(\tau), \quad W\left(-\frac{1}{\tau}\right) = W(\tau)$$

Set $\tilde{W}(\tau) = W(\tau)\,\eta^8(\tau)$

From (I. 4.4.1) we have:

$$\eta^8(\tau + 1) = e^{2\pi i/3}\ \eta^8(\tau),\ \eta^8\left(-\frac{1}{\tau}\right) = \tau^4\eta^8(\tau)$$

Thus $\tilde{W}(\tau + 1) = W(\tau + 1)\ \eta^8(\tau + 1)$

$$= e^{4\pi i/3}\ W(\tau)\ e^{2\pi i/3}\ \eta^8(\tau)$$

$$= W(\tau)\ \eta^8(\tau)$$

$$= \tilde{W}(\tau)$$

Also $\tilde{W}\left(-\frac{1}{\tau}\right) = W\left(-\frac{1}{\tau}\right)\eta^8\left(-\frac{1}{\tau}\right)$

$$= W(\tau)\ \tau^4\ \eta^8(\tau)$$

$$= \tau^4\tilde{W}(\tau)$$

So, $\tilde{W}(\tau)$ is a weakly modular function of weight 4 for $\hat{\Gamma}$.

Now:

$$\tilde{W}(\tau) = \left[f^8(\tau)f_1^8(\tau) + f^8(\tau)\ f_2^8(\tau) - f_1^8(\tau)\ f_2^8(\tau)\right]\eta^8(\tau) - \frac{3}{4\pi^4}g_2(\tau)$$

Hence $\tilde{W}(\tau)$ is holomorphic on $\mathcal{H}^*$.

Therefore $\tilde{W}(\tau)$ is a modular form, of weight 4, for $\hat{\Gamma}$.

If we prove that $\tilde{W}(\tau)$ is actually a cusp form, then, by (Th. I. 3.5.2 (i)), we deduce that $\tilde{W}(\tau) = 0$, and thus $W(\tau) = 0$, which completes the proof of (I. 4.6.6).

Therefore, it suffices to prove that $\tilde{W}(\tau)$ is a cusp form. So, it is enough to prove that $\tilde{W}(\tau)$ tends to zero as $\tau \to i\infty$ (or $q \to 0$). Now using the formulae (I. 4.6.5), (I. 4.6.7) of the (Lem. I. 4.6.4), we may write:

$$\tilde{W}(\tau) = \left[\frac{2^4}{f_2^8(\tau)} + f_2^{16}(\tau)\right] \cdot \eta^8(\tau) - \frac{3}{4\pi^4}g_2(\tau)$$

and so

$$\tilde{W}(\tau) = \frac{\eta^{16}(\tau)}{\eta^8(\tau)} + f_2^{16}(\tau)\eta^8(\tau) - \frac{3}{4\pi^4}\ g_2(\tau) \qquad \text{(I. 4.6.8)}$$

Since $f_2(\tau) = \sqrt{2}\ \frac{\eta(2\tau)}{\eta(\tau)}$, and $\eta^8(\tau)$ is a cusp form we deduce that $f_2^{16}(\tau)\ \eta^8(\tau) \to 0$, as $\tau \to i\infty$.

Also $\frac{\eta^{16}(\tau)}{\eta^8(\tau)} \to 1$, as $\tau \to i\infty$.

From the q-expansion of $g_2(\tau)$, given by (I. 4.1.2), we deduce that $g_2(\tau) \to \frac{4\pi^4}{3}$, as $\tau \to i\infty$.

Therefore, from (I. 4.6.8) we have $\tilde{W}(\tau) \longrightarrow 0$, as $\tau \longrightarrow i\infty$, and this completes the proof of (I. 4.6.6).

From the (Lem I. 4.6.4), we deduce the following theorem.

Theorem (Th. I. 4.6.9)

The functions $f^8(\tau)$, $-f_1^8(\tau)$, $-f_2^8(\tau)$ are the roots of the cubic equation $X^3 - \gamma_2(\tau)x - 16 = 0$.

Theorem (Th. I. 4.6.10)

The function $f(\tau)$ is modular of weight 0, for a congruence subgroup G^f of index 72 in $\hat{\Gamma}$.

The functions $f_1(\tau)$, $f_2(\tau)$ are also modular of weight 0, for $G^{f_1} = T\, G^f\, T^{-1}$, $G^{f_2} = S^{-1}\, T\, G^f\, T^{-1}\, S$, respectively.

In particular, the functions $f(\tau)$, $f_1(\tau)$, $f_2(\tau)$ are invariant under $\hat{\Gamma}(48)$, and have Fourier expansions at each cusp of $\hat{\Gamma}(48)$ with coefficients lying in the cyclotomic field $\mathbb{Q}(e^{2\pi i/48})$.

Proof

First, we take the congruence subgroups $\Gamma_S(2)$, and Γ^3, defined by:

$$\Gamma_S(2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) : (a - d) + (b - c) \equiv 0 \pmod 2 \right\},$$

$$\Gamma^3 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) : ab + cd \equiv 0 \pmod 3 \right\}$$

We get all the information we need about these groups from (Rankin, [35] , p.p. 29-33, and Table 3 in p.p. 63, where $\Gamma_S(2)$ is denoted by $\Gamma_V(2)$).

We quote that:

$\hat{\Gamma}(2)$ is a normal subgroup of $\hat{\Gamma}_S(2)$ of index 2, and $\hat{\Gamma}_S(2)$ is a (not normal) subgroup of $\hat{\Gamma}$ of index 3. Also, that $\hat{\Gamma}_S(2) = \langle S, T^2 \rangle$, and $\hat{\Gamma}(2) = \langle T^2, S\, T^2\, S \rangle$, and therefore it is clear that $\hat{\Gamma}_S(2) = \langle \hat{\Gamma}(2), S \rangle$.

We have also that:

$\hat{\Gamma}(3)$ is a normal subgroup of $\hat{\Gamma}^3$ of index 4, and $\hat{\Gamma}^3$ is a normal subgroup of $\hat{\Gamma}$ of index 3. Also, that $\hat{\Gamma}^3 = \langle S, STST^{-1}S, T^{-1}S\, T \rangle$.

Since (I. 4.6.3), we have:

$$\begin{aligned} f\,T(\tau) &= e^{-\pi i/24} f_1(\tau) \\ f_1 T(\tau) &= e^{-\pi i/24} f(\tau) \\ f\,S(\tau) &= f(\tau) \end{aligned} \qquad \text{(I.4.6.11)}$$

For the 3^{rd} power of f, since (I. 4.6.11), we get:

$$\begin{aligned} f^3\,T(\tau) &= e^{-\pi i/8} f_1^3(\tau) \\ f_1^3\,T(\tau) &= e^{-\pi i/8} f^3(\tau) \\ f^3\,S(\tau) &= f^3(\tau) \end{aligned} \qquad \text{(I. 4.6.12)}$$

and hence the action of $\hat{\Gamma}(2)$ on f^3 is given by

$$\begin{aligned} f^3\,T^2(\tau) &= e^{7\pi i/4} f^3(\tau) \quad , \\ f^3\,ST^2S(\tau) &= e^{7\pi i/4} f^3(\tau) \end{aligned} \qquad \text{(I. 4.6.13)}$$

Let V_{f^3} be the $\mathbb{C}$-vector space generated by the images of f^3 under $\hat{\Gamma}(2)$. Since $\hat{\Gamma}(2) = \langle T^2, ST^2S \rangle$, and (I. 4.6.13), we have $V_{f^3} = \langle f^3 \rangle_{\mathbb{C}}$, that is V_{f^3} is of dimension 1.

Now, V_{f^3} affords a group representation of $\hat{\Gamma}(2)$,

$$\rho_{f^3} : \hat{\Gamma}(2) \longrightarrow \mathrm{Aut}\,(V_{f^3})$$

Also, since V_{f^3} is of dimension 1, the character

$$\chi_{\rho_{f^3}} : \hat{\Gamma}(2) \longrightarrow \mathbb{C}^{\times}$$

is a group homomorphism, and is defined by its image on the generators of $\hat{\Gamma}(2)$, that is ,

$$\chi_{\rho_{f^3}}(T^2) = e^{7\pi i/4} \text{ , and } \chi_{\rho_{f^3}}(ST^2S) = e^{7\pi i/4}$$

Thus, we have also, $im(\chi_{\rho_{f^3}}) \cong \mathbb{Z}_8$.

Since, it is clear that the function f^3 is invariant under the Kernel of $\chi_{\rho_{f^3}}$, we intend to identify that.

Define the map

$$\varphi : \hat{\Gamma}(2) \longrightarrow (\mathbb{Z}_8, +) \text{ by}$$

$$\varphi \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \frac{c-b}{2} \cdot a \pmod 8$$

It is not difficult to prove that φ is a group epimorphism.

Also, note that

$$\mathrm{Ker}\,\tilde{\varphi} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \hat{\Gamma}(2) \;:\; b \equiv c \pmod{16} \right\}$$

and hence $\mathrm{Ker}\,\tilde{\varphi} \subseteq \hat{\Gamma}(48)$

Now, the map

$$\psi : \mathbb{Z}_8 \longrightarrow \mathbb{C}^{\times}$$

defined by:

$$\psi(n) = e^{n\pi i/4}$$

is a group homomorphism, and the composite map

$$\psi \circ \tilde{\varphi} : \quad \hat{\Gamma}(2) \longrightarrow \mathbb{C}^{\times}$$

is identical with the $\chi_{P_{f^3}}$.

Thus, we proved that the function f^3 is invariant under the group:

$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \hat{\Gamma}(2) \quad : \; b \equiv c \pmod{16} \right\}$$

and in fact $G \supseteq \hat{\Gamma}(48)$. Also, since $\hat{\Gamma}(2)/G \cong \mathbb{Z}_8$, $[\hat{\Gamma}(2) : G] = 8$

and hence $[\hat{\Gamma} : G] = 48$.

Now, since the function f^3 is invariant under S, it is also

under the subgroup generated by G, and S, namely

$$G_S = \langle G, S \rangle$$

Since $\langle G, S \rangle / G \cong \langle \hat{\Gamma}(2), S \rangle / \hat{\Gamma}(2)$

$$G_S / G \cong \hat{\Gamma}_S(2) / \hat{\Gamma}(2)$$

and hence $[G_S : G] = 2$, therefore

$$[\hat{\Gamma} : G_S] = 24.$$

Now we look at the 8th power of f.

By the (Th. I. 4.6.9), we have:

$$f^8(\tau) = \frac{f^{24}(\tau) - 16}{\gamma_2(\tau)} \qquad \text{(I. 4.6.14)}$$

From (I. 4.6.11)

$$f^{24} T^2 (\tau) = f^{24}(\tau)$$

$$f^{24} S (\tau) = f^{24}(\tau)$$

Therefore, the function f^{24} is invariant under $\hat{\Gamma}_S(2)$.

For the function γ_2 we deduce from (I. 4.5.4) that:

$$\gamma_2 T\ (\tau) = e^{4\pi i/3}\ \gamma_2(\tau)\ ,$$
$$\gamma_2 S\ (\tau) = \gamma_2(\tau)\ . \qquad \text{(I. 4.6.15)}$$

Now from (I. 4.6.15), it is easily verified that γ_2 is invariant under the generators of the subgroup $\hat{\Gamma}^3$, and hence invariant under the action of $\hat{\Gamma}^3$. Therefore, in view of (I. 4.6.14), the function $f^8(\tau)$ is invariant under the subgroup $\hat{\Gamma}_S(2) \cap \hat{\Gamma}^3$.

We see from (I. 4.6.1), that the function $f(\tau)$ is non-zero on $\mathfrak{H}$.

Note, that the function f written as

$$\frac{(f^8)^2}{(f^3)^5}$$

is invariant under the intersection of G_S , and $\hat{\Gamma}_S(2) \cap \hat{\Gamma}^3$, and since $G_S \leq \hat{\Gamma}_S(2)$, $G_S \cap \left(\hat{\Gamma}_S(2) \cap \hat{\Gamma}^3\right) = G_S \cap \hat{\Gamma}^3$.

Now, since $\hat{\Gamma}^3$ is a normal subgroup of $\hat{\Gamma}$, by the isomorphism theorem

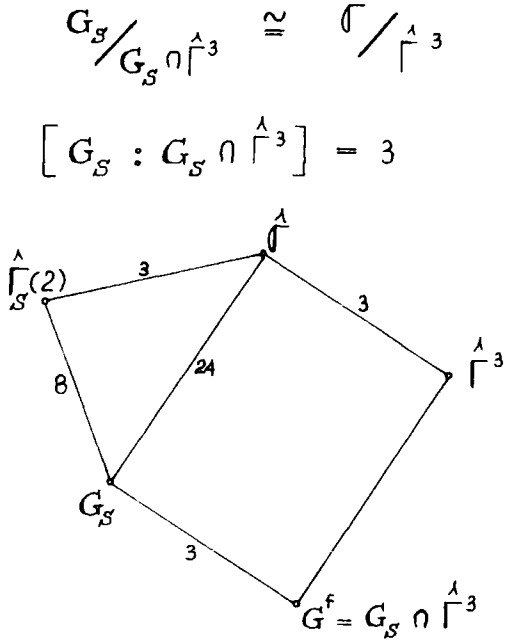
$$G_S / G_S \cap \hat{\Gamma}^3 \cong G_S \cdot \hat{\Gamma}^3 / \hat{\Gamma}^3 ,$$

and hence

$$G_S / G_S \cap \hat{\Gamma}^3 \cong \hat{\Gamma} / \hat{\Gamma}^3 ,$$

and so

$$\left[G_S : G_S \cap \hat{\Gamma}^3 \right] = 3 .$$



Therefore, the function $f(\tau)$ is invariant under $G_S \cap \hat{\Gamma}^3$ which is of index 72 in $\hat{\Gamma}$, and since $G_S \supseteq \hat{\Gamma}(48)$, and $\hat{\Gamma}^3 \supseteq \hat{\Gamma}(48)$ the function $f(\tau)$ is also invariant under $\hat{\Gamma}(48)$. From (I. 4.6.2), $f(\tau)$ is holomorphic on $\mathfrak{H}$.

Therefore $f(\tau)$ is a weakly modular function of weight 0 for $G^f = G_S \cap \hat{\Gamma}^3$.

From (I. 4.6.1), $f(\tau)$ is meromorphic at $i\infty$.

Note that in view of (Th. I. 3.1.5), and (I. 4.6.3), the function:

$$f|[T^{-1}]_0(\tau) = f\left(T^{-1}(\tau)\right) = e^{\pi i/24} f_1(\tau)$$

is a weakly modular of weight 0 for $G^{f_1} = T G^f T^{-1}$.

Also, the function

$$f_1|[S^{-1}]_0(\tau) = f_1\left(S(\tau)\right) = f_2(\tau)$$

is a weakly modular of weight 0 for $G^{f_2} = S^{-1} T G^f T^{-1} S$.

From (I. 4.6.1), $f_1(\tau)$ and $f_2(\tau)$ are also meromorphic at infinity.

Now, we prove that the function $f(\tau)$ is meromorphic at each rational cusp of G^f, for $\mathfrak{H}^*$. For, suppose that $-\frac{d}{c}$, $c \neq 0$, $(c, d) = 1$ is a rational cusp of G^f, for $\mathfrak{H}^*$, and the transformation $\rho \in \hat{\Gamma}$ sends $-\frac{d}{c}$ to $i\infty$. Then, in view of (Def. I. 3.1.8), and the formulae (I. 4.6.3), the function:

$$f|[\rho^{-1}]_0(\tau) = f(\rho^{-1}(\tau)) = \xi F(\tau)$$

where $F = f$, f_1 or f_2 and ξ is a 48th root of unity. Now since $\xi F(\tau)$ is meromorphic at $i\infty$, $f(\tau)$ is meromorphic at $-\frac{d}{c}$. Hence, $f(\tau)$ is a modular function of weight 0 for $G^f = G_S \cap \hat{\Gamma}^3$. Similarly, we can also prove that $f_1(\tau)$, $f_2(\tau)$ are meromorphic at all rational cusps of G^{f_1}, G^{f_2}, for $\mathfrak{H}^*$, respectively. Hence $f_1(\tau)$, $f_2(\tau)$ are modular functions of weight 0, for G^{f_1}, G^{f_2}, respectively.

Now since $\hat{\Gamma}(48)$ is a normal subgroup of $\hat{\Gamma}$, $\hat{\Gamma}(48) \cdot T = T \cdot \hat{\Gamma}(48)$, and so $\hat{\Gamma}(48)\, T \subseteq T\, G^f$. Hence $\hat{\Gamma}(48) \subseteq T\, G^f\, T^{-1}$, that is $\hat{\Gamma}(48) \subseteq G^{f_1}$. Similarly $\hat{\Gamma}(48) \subseteq G^{f_2}$.

Therefore $f_1(\tau)$, $f_2(\tau)$ are invariant under $\hat{\Gamma}(48)$. It is clear, from (I. 4.6.1), that the functions $f(\tau)$, $f_1(\tau)$, $f_2(\tau)$ have Fourier expansions at $i\infty$ with coefficients lying in $\mathbb{Q}(e^{2\pi i/24})$. Now, in view of (Def. I. 3.1.8), and (I. 4.6.3), these functions

have also Fourier expansions at all rational cusps of $\hat{\Gamma}(48)$ with coefficients lying in $\mathbb{Q}(e^{2\pi i/48})$.

Therefore the theorem holds.

Theorem (Th. I. 4.6.16)

The functions $f^{24}(\tau)$, $f_1^{24}(\tau)$, $f_2^{24}(\tau)$ are modular of weight 0 for $\hat{\Gamma}(2)$. In particular, each of them has Fourier expansions at all cusps of $\hat{\Gamma}(2)$ for $\mathfrak{H}^*$ with coefficients lying in $\mathbb{Q}$.

Proof

From (I. 4.6.3) the functions $f^{24}(\tau)$, $f_1^{24}(\tau)$, $f_2^{24}(\tau)$ are all invariant under the generators T^2, ST^2S of $\hat{\Gamma}(2)$, and so they are invariant under $\hat{\Gamma}(2)$.

In view of (I. 4.6.1) these functions are holomorphic on $\mathfrak{H}$. Also the first two are meromorphic at $i\infty$ and the last holomorphic at $i\infty$ and indeed vanishes there. The cusps of $\hat{\Gamma}(2)$ are $\{i\infty, 0, 1\}$, and the transformations S, ST^{-1} send 0, 1 to $i\infty$, respectively. From (I. 4.6.3), we deduce that

$$f^{24}S^{-1}(\tau) = f^{24}(\tau) \quad , \quad f_1^{24}S^{-1}(\tau) = f_2^{24}(\tau) \quad , \quad f_2^{24}S^{-1}(\tau) = f_1^{24}(\tau)$$
$$f^{24}TS^{-1}(\tau) = -f_2^{24}(\tau), \quad f_1^{24}TS^{-1}(\tau) = -f^{24}(\tau) \quad , \quad f_2^{24}TS^{-1}(\tau) = f_1^{24}(\tau)$$

(I. 4.6.17)

We denote by $F(\tau)$ any of thefunctions $f^{24}(\tau)$, $f_1^{24}(\tau)$, $f_2^{24}(\tau)$. In view of the (Def. I. 3.1.8), we have:

$$F|[S^{-1}]_0(\tau) = F(S^{-1}(\tau)) \quad ,$$
$$F|[TS^{-1}]_0(\tau) = F(TS^{-1}(\tau)) \, .$$

From the above, and (I. 4.6.17), it is clear that $F(\tau)$ is meromorphic at all the rational cusps of $\hat{\Gamma}(2)$ for $\mathfrak{H}^*$.

Also, from (I. 4.6.17), we deduce that $F(\tau)$ has a Fourier expansion at each cusp with coefficients in $\mathbb{Q}$. So the theorem holds.

5. The Modular Polynomial

In this paragraph we introduce the notion of the modular polynomial, in order to prove later on the following fundamental theorem.

"If τ is an imaginary quadra tic number lying on $\mathfrak{H}$, then $j(\tau)$ is an algebraic integer."

Let n be any positive integer.

We denote by:

Δ_n: The set of all 2 x 2 matrices with entries in $\mathbb{Z}$ and determinant n .

Δ_n^*: The subset of Δ_n containing only primitive elements, that is, of the type $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with (a, b, c, d) = 1.

5.1 A Determination of Δ_n^*

Lemma (Lem. I. 5.1.1)

$\forall \alpha \in \Delta_n^*$, $\forall \mu \in \Gamma(1)$ we have $\alpha\mu \in \Delta_n^*$, $\mu\alpha \in \Delta_n^*$

Proof

Obviously $\alpha\mu \in \Delta_n$

Suppost that $\alpha\mu \notin \Delta_n^*$. Therefore, there is an integer d, $d > 1$, such that $\alpha\mu = d\beta$, where $\beta \in \Delta_n^*$.

Hence $\frac{1}{d}\alpha = \beta\mu^{-1}$ - contradiction.

Therefore $\alpha\mu \in \Delta_n^*$. Similarly, $\mu\alpha \in \Delta_n^*$.

Now, since (Lem I.5.1.1) holds, we can define an action, either left or right, of the homogeneous group $\Gamma(1)$ on the set Δ_n^*. Thus, the orbit of an element $\alpha \in \Delta_n^*$, under the left action, is the right coset $\Gamma(1)\alpha$.

In the following, by "an action", we mean a "left action".

Also, we say that the elements $\alpha, \alpha_1 \in \Delta_n^*$ are equivalent under $\Gamma(1)$, or they are congruent mod $\Gamma(1)$ and write

$$\alpha \overset{\Gamma(1)}{\sim} \alpha_1 \qquad \text{or} \qquad \alpha \equiv \alpha_1 \pmod{\Gamma(1)} ,$$

if and only if, they lie in the same orbit of Δ_n^* under $\Gamma(1)$.

By considering integer row and column reduction we can prove the following two lemmas:

Lemma (Lem. I. 5.1.2)

For every $\alpha \in \Delta_n^*$, there are $\mu, \mu' \in \Gamma(1)$, such that

$$\mu \alpha \mu' = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}$$

Thus, $\Delta_n^* = \Gamma(1) \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Gamma(1)$, and consequently, the homogeneous group $\Gamma(1)$ acts left transitevely on the left $\Gamma(1)$ cosets, and also right transitevely on the right $\Gamma(1)$ cosets of Δ_n^*.

Lemma (Lem. I. 5.1.3)

Every matrix $\alpha \in \Delta_n^*$ is congruent mod $\Gamma(1)$ to a unique triangular matrix:

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

where $0 < a$, $0 \leq b < d$, $ad = n$, and $(a, b, d) = 1$.

Thus $\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : 0 < a,\ 0 \leq b < d,\ ad = n,\ (a, b, d) = 1 \right\}$ is a set of representatives for the cosets of $\Gamma(1)$ in Δ_n^*.

Theorem (Th. I. 5.1.4)

The number $\psi(n)$ of equivalence classes of Δ_n^* under the action of $\Gamma(1)$ is given by:

$$\psi(n) = n \prod_{p \mid n} \left(1 + \frac{1}{p}\right)$$

Proof

We prove first that $\psi(p) = p + 1$.

By (Lem. I. 5.1.3) an arbitrary chosen $\alpha \in \Delta_p^*$ is equivalent either to $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ or to $\begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix}$, where $0 \leq b < p$. Therefore there are exactly $p + 1$ equivalence classes in Δ_p^*, that is, $\psi(p) = p + 1$.

Now we prove the theorem for any positive integer n.

It suffices to count all inequivalent matrices of the type

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

where $0 < a$, $0 \leq b < d$, $ad = n$, and $(a, b, d) = 1$.

Suppose that d is fixed, and so does $a = \frac{n}{d}$. We set $(a,d) = e$ and count b's. Put $d = ek$, and $\mathcal{A} = \{ 0, 1, 2, \dots, e, e+1, e+2, \dots, 2e, 2e+1, \dots, 3e, \dots, ke \}$. It is enough to find all those elements of $\mathcal{A}$ which are relatively prime to e.

We know that among ν consecutive integers there are just $\varphi(\nu)$ integers relatively prime to ν. The set $\mathcal{A}$ contains k such sets and so contains $k\varphi(e)$ such elements. Now, since d runs through all divisors of n, we have :

$$\psi(n) = \sum_{d|n} \frac{d}{e} \varphi(e)$$

Note, now, that $\psi(n)$ is a multiplicative arithmetic function. For, if $(n_1, n_2) = 1$, we have:

$$\begin{aligned}
\psi(n_1)\psi(n_2) &= \sum_{d_1|n_1} \frac{d_1}{e_1} \varphi(e_1) \sum_{d_2|n_2} \frac{d_2}{e_2} \varphi(e_2) \\
&= \sum_{\substack{d_1|n_1 \\ d_2|n_2}} \frac{d_1 d_2}{e_1 e_2} \varphi(e_1)\varphi(e_2) \\
&= \sum_{\substack{d_1|n_1 \\ d_2|n_2}} \frac{d_1 d_2}{e_1 e_2} \varphi(e_1 e_2) \qquad \text{(since, } \varphi \text{ is multiplicative)} \\
&= \sum_{d_1 d_2 | n_1 n_2} \frac{d_1 d_2}{e_1 e_2} \varphi(e_1 e_2) \\
&= \psi(n_1 n_2)
\end{aligned}$$

This last result suffices for our study of ψ to the case when $n = p^r$ (p prime, $r > 0$).

We have:
$$\begin{aligned}
\psi(p^r) &= \sum_{d|p^r} \frac{d}{(a,d)} \varphi(a,d) \\
&= \sum_{\mu=0}^{r} \frac{p^\mu}{(p^{r-\mu}, p^\mu)} \varphi(p^{r-\mu}, p^\mu) \\
&= 1 + p^r + \sum_{\mu=1}^{r-1} \varphi(p^\mu) \\
&= 1 + p^r + p^{r-1} - 1 \\
&= p^r + p^{r-1} \\
&= p^r \left(1 + \frac{1}{p}\right)
\end{aligned}$$

for which the conclusion follows.

5.2 The Modular Polynomial

In the following we denote by

$$\alpha_1 , \alpha_2 , \ldots , \alpha_{\psi(n)}$$

a complete system of inequivalent representatives of Δ_n^* with respect to the modular group $\hat{\Gamma}$.

By the (Th. I. 4.3.2), the functions $j\circ\alpha_1 , j\circ\alpha_2 , \ldots , j\circ\alpha_{\psi(n)}$ are distinct. Also, by the (Lem. I. 5.1.2), the modular group $\hat{\Gamma}$ acts transitively on the set $\{ j\circ\alpha_i : 1 \leq i \leq \psi(n) \}$.

Definition (Def. I. 5.2.1)

Let $\mathcal{M}(\mathfrak{H}^*)$ be the field of meromorphic functions on $\mathfrak{H}^*$.

The polynomial $\Phi_n(X) \in \mathcal{M}(\mathfrak{H}^*)[X]$ given by

$$\Phi_n(X) = \prod_{i=1}^{\psi(n)} (X - j\circ\alpha_i)$$

is called the modular polynomial of order n.

Theorem (Th. I. 5.2.2) The coefficients of the modular polynomial

$$\Phi_n(X) = \prod_{i=1}^{\psi(n)} (X - j\circ\alpha_i)$$

are polynomials in j with integral coefficients.

Proof

Write $j(\tau) = \sum_{n=1}^{\infty} c_n q^n$, $q = e^{2\pi i\tau}$, $c_n \in \mathbb{Z}$, $c_{-1} = 1$

Each α_i ($1 \leq i \leq \psi(n)$) may be chosen as $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, where

$$0 < a,\ 0 \leq b < d ,\ ad = n,\ (a, b, d) = 1 \qquad (1)$$

Therefore $\alpha_i(\tau) = \dfrac{a\tau + b}{d}$.

In order to find the Fourier expansion of $j\circ\alpha_i$ we replace τ by $\dfrac{a\tau + b}{d}$ and so q becomes

$$e^{2\pi i \frac{a\tau+b}{d}} = e^{2\pi i\tau \frac{a}{d}} \cdot e^{2\pi i \frac{b}{d}}$$

Set $\zeta_d = e^{2\pi i/d}$, and so q becomes $q^{a/d}\,\zeta_d^b$

Therefore we may write $\Phi_n(X)$

$$\text{as} \quad \prod_{\substack{a,b,d \\ \text{as in (1)}}} \left(X - \sum_{m=-1}^{\infty} c_m q^{\frac{a}{d}m} \zeta_d^{bm} \right)$$

and a direct calculation of this product gives:

$$\Phi_n(X) = \sum_{\mu=0}^{\psi(n)} \left(\sum_{\nu=-\psi(n)}^{\infty} C_{\mu\nu}\, q^{\nu} \right) X^{\mu}$$

where $C_{\mu\nu} = \sum_{k=0}^{n-1} m_k e^{\frac{2\pi i}{n} k}$, with rational integers m_k .

On the other hand the coefficients of $\Phi_n(X)$ are the elementary symmetric functions of $j\circ\alpha_i$ and indeed modular functions themselves. Now, since $\hat{\Gamma}$ acts transitively on $j\circ\alpha_i$ the coefficients of $\Phi_n(X)$ are invariant under $\hat{\Gamma}$. Also, since j and each α_i are holomorphic on $\mathcal{H}$, so is $j\circ\alpha_i$ and hence are the coefficients of $\Phi_n(X)$.

Therefore, by (Th. I. 4.3.3 (ii)), the coefficients of $\Phi_n(X)$ are polynomials in j with coefficients in $\mathbb{Z}[C_{\mu\nu}]$, and so it is enough to prove that the $C_{\mu\nu}$ are rational integers.

So far we have that $C_{\mu\nu}$ are algebraic integers in the cyclotomic field $\mathbb{Q}(e^{2\pi i/n})$ and therefore it suffices to prove that the $C_{\mu\nu}$ are rational.

If one replaces b by bk, where (n, k) = 1, the formula for $\Phi_n(X)$ is valid, and so the $C_{\mu\nu}$ remain unchanged. Such a substitution is the result of a $\mathbb{Q}$ -automorphism of the cyclotomic field $\mathbb{Q}(e^{2\pi i/n})$ given by

$$e^{\frac{2\pi i}{n}} \longrightarrow e^{\frac{2\pi i}{n} k} \qquad , (k, n) = 1$$

and therefore $C_{\mu\nu} \in \mathbb{Q}$. This completes the proof.

Thus: $$\Phi_n(X) \in \mathbb{Z}[j][X]$$

so we may view $\Phi_n(X)$ as a polynomial in the two independent variables X and j with integer coefficients and we write:

$$\Phi_n(X) = \Phi_n(X, j) \in \mathbb{Z}[X, j]$$

Lemma (Lem. I. 5.2.3)

If n is not a square, then $\Phi_n(j, j)$ is a polynomial in j of degree >1 and with leading coefficient ± 1.

Proof

Write $$\Phi_n(j, j) = \prod_{i=1}^{\psi(n)} (j - j\circ\alpha_i) = \prod_{\substack{(a,b,d)=1 \\ ad=n \\ 0<a \\ 0\le b<d}} \left(\frac{1}{q} + \ldots - \frac{1}{\zeta_d^b\, q^{a/d}} - \ldots \right) \quad (*)$$

Since n is not a square, and ad = n, we have $a \neq d$. Therefore there

is no cancellation in the polar term in each bracket on the right hand side of (*) and furthermore, the leading coefficient of each bracket q-expansion is a root of unity . Therefore the q-expansion for $\Phi_n(j, j)$ starts with

$$\frac{c_m}{q^m} + \cdots$$

with C_m an integer and also a root of unity and so we must have $C_m = \pm 1$. This result completes the proof.

Theorem (Th. I. 5.2.4)

If τ is an imaginary quadratic number lying on $\mathfrak{H}$, then $j(\tau)$ is an algebraic integer.

Proof

Let $\tau \in K$, where K is an imaginary quadratic field and z be an algebraic integer such that

$$K = \mathbb{Q}(z) \quad , \text{ and } R_o = \text{int } K = \mathbb{Z}[z]$$

We can always find an element $W \in R_o$ with norm over $\mathbb{Q}$ a square-free integer.

For if $K = \mathbb{Q}(i)$, we take $W = 1 + i$ and if $K = \mathbb{Q}(\sqrt{-d})$, where d is a square-free rational integer > 1, we take $w = \sqrt{-d}$.

Now, we can find a, b, c, $d \in \mathbb{Z}$, with (a, b, c, d) = 1 so that

$$wz = az + b$$

$$w = cz + d$$

Note that $\begin{vmatrix} a-w & b \\ c & d-w \end{vmatrix} = 0$ gives $w^2 - (a+d)w + ad-bc = 0$

and therefore $N_{K/\mathbb{Q}}(w) = ad-bc$.

So in that case, put ad-bc = n and therefore n is not a square.

Put $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then $\alpha \in \Delta_n^*$, and $\alpha(z) = z$.

Let $\alpha_1, \alpha_2, \ldots, \alpha_{\psi(n)}$ be a complete system of inequivalent representatives of Δ_n^* .

We must have $\alpha \overset{\hat{\Gamma}}{\sim} \alpha_i$ for some i: $1 \leq i \leq \psi(n)$ and hence $\exists \rho \in \hat{\Gamma}$ such that $\alpha = \rho \alpha_i$

Therefore $j(z) = j(\alpha(z)) = (j \circ \rho)(\alpha_i(z)) = j \circ \alpha_i(z)$.

Hence $j(z)$ is a zero of the polynomial $\Phi_n(j, j)$ which lies in $\mathbb{Z}[j]$

and has leading coefficient 1 according to the (Th. I. 5.2.2), and therefore $j(z)$ is an algebraic integer. Now, we prove that $j(\tau)$ is also an algebraic integer. Since $\tau \in \mathbb{Q}(z)$, $\exists$ $r, s \in \mathbb{Q}$ such that $\tau = r z + s$, that is $\tau = \beta(z)$ for some primitive $\beta \in GL_2^+(\mathbb{Q})$. Since $j \circ \beta$ is integral over $\mathbb{Z}[j]$ it follows that $j(\tau) = j \circ \beta(z)$ is integral over $\mathbb{Z}[j(z)]$, and hence $j(\tau)$ is also an algebraic integer, as required.

Theorem (Th. I. 5.2.5)

For any rational prime $p \geq 7$, $\gamma_2\left(\frac{-3+\sqrt{-p}}{2}\right)$ is a real algebraic integer less than zero.

First we prove the following lemma:

Lemma (Lem. I. 5.2.6)

$$\gamma_2\left(\frac{\tau-3}{2}\right) = \frac{256}{f^{16}(\tau)} - f^8(\tau) \qquad \text{(I. 5.2.6)}$$

Proof of the Lemma:

Since $-f_2^8(\tau)$ is a root of the equation

$$x^3 - \gamma_2(\tau)x - 16 = 0$$

we have: $\gamma_2(\tau) = f_2^{16}(\tau) + \frac{16}{f_2^8(\tau)}$

and so, $$\gamma_2\left(\frac{\tau-3}{2}\right) = 16 f_2^{-8}\left(\frac{\tau-3}{2}\right) + f_2^{16}\left(\frac{\tau-3}{2}\right) \qquad \text{(I. 5.2.7)}$$

Now express $f_2\left(\frac{\tau-3}{2}\right)$ in terms of $f(\tau)$.

Since $$f_2(\tau) = \sqrt{2}\,\frac{\eta(2\tau)}{\eta(\tau)}$$ (see (I. 4.6.2))

we have: $$f_2\left(\frac{\tau-3}{2}\right) = \sqrt{2}\,\frac{\eta(\tau-3)}{\eta\left(\frac{\tau-3}{2}\right)} \qquad \text{(I. 5.2.8)}$$

Since $\eta(\tau) = e^{-2\pi i/24}\,\eta(\tau+1)$

we have: $$\eta\left(\frac{\tau-3}{2}\right) = e^{-2\pi i/24}\,\eta\left(\frac{\tau-1}{2}\right)$$

$$= e^{-2\pi i/24}\, e^{-2\pi i/24}\,\eta\left(\frac{\tau+1}{2}\right)$$

Also: $$\eta(\tau-3) = e^{-2\pi i/24}\,\eta(\tau-2)$$

$$= e^{-2\pi i/24}\, e^{-2\pi i/24}\,\eta(\tau-1)$$

$$= e^{-2\pi i/24}\, e^{-2\pi i/24}\, e^{-2\pi i/24}\,\eta(\tau)$$

Therefore $$\frac{\eta(\tau-3)}{\eta(\frac{\tau-3}{2})} = e^{-2\pi i/24}\cdot\frac{\eta(\tau)}{\eta(\frac{\tau+1}{2})}$$

and since (I. 4.6.2),

We have, $$\frac{\eta(\tau-3)}{\eta(\frac{\tau-3}{2})} = \frac{e^{-\pi i/8}}{f(\tau)}$$

and hence (I. 5.2.8) gives:

$$f_2(\frac{\tau-3}{2}) = \frac{\sqrt{2}\, e^{-\pi i/8}}{f(\tau)} \qquad \text{(I. 5.2.9)}$$

Finally, from (I. 5.2.7), and (I. 5.2.9) the desired (I. 5.2.6) follows.

Proof of the Theorem

Setting $\tau = \sqrt{-p}$ in (I. 5.2.6) we take:

$$\gamma_2(\frac{-3+\sqrt{-p}}{2}) = \frac{256}{f^{16}(\sqrt{-p})} - f^8(\sqrt{-p}) \qquad \text{(I. 5.2.10)}$$

where, as usual $f(\sqrt{-p}) = q^{-1/48}\prod_{n=1}^{\infty}(1+q^{n-\frac{1}{2}})$ and $q = e^{-2\pi\sqrt{p}}$

Note, since $q = e^{-2\pi\sqrt{p}} \in \mathbb{R}$, $f(\sqrt{-p}) \in \mathbb{R}$, and hence (I .5.2.10) implies $\gamma_2(\frac{-3+\sqrt{-p}}{2}) \in \mathbb{R}$

Now, since $$\gamma_2^3(\frac{-3+\sqrt{-p}}{2}) = j(\frac{-3+\sqrt{-p}}{2})$$

and $j(\frac{-3+\sqrt{-p}}{2})$ is an algebraic integer (from Th. I. 5.2.4) we deduce $\gamma_2(\frac{-3+\sqrt{-p}}{2})$ is an algebraic integer, and since $\gamma_2(\frac{-3+\sqrt{-p}}{2}) \in \mathbb{R}$, we have:

$\gamma_2(\frac{-3+\sqrt{-p}}{2})$ is a real algebraic integer.

Now we prove that $\gamma_2\left(\frac{-3+\sqrt{-p}}{2}\right)$ is negative.

Since $q = e^{-2\pi\sqrt{p}} > 0$, $f(\sqrt{-p}) > q^{-1/48}$

Therefore $$\gamma_2\left(\frac{-3+\sqrt{-p}}{2}\right) < 256\, q^{1/3} - q^{-1/6} \qquad (I.5.2.11)$$

So $$\gamma_2\left(\frac{-3+\sqrt{-p}}{2}\right) < q^{1/3}\left(2^8 - e^{\pi\sqrt{p}}\right)$$

and so $$\gamma_2\left(\frac{-3+\sqrt{-p}}{2}\right) < q^{1/3}\left(e^8 - e^{\pi\sqrt{7}}\right)$$

and since $\pi\sqrt{7} > 8$ we deduce that $\gamma_2\left(\frac{-3+\sqrt{-p}}{2}\right) < 0$

Theorem (Th. I. 5.2.12)

For any rational prime $p \geq 7$, $j\left(\frac{1+\sqrt{-p}}{2}\right)$ is a real algebraic integer less than zero.

Proof

By the (Th. I. 5.2.5), and since $j\left(\frac{-3+\sqrt{-p}}{2}\right) = \gamma_2^3\left(\frac{-3+\sqrt{-p}}{2}\right)$ we have that $j\left(\frac{-3+\sqrt{-p}}{2}\right)$ is a real algebraic integer less than zero. Now, since $j(\tau)$ is invariant under $\hat{\Gamma}$, we have $j\left(\frac{-3+\sqrt{-p}}{2}\right) = j\left(\frac{-3+\sqrt{-p}}{2}+2\right) = j\left(\frac{1+\sqrt{-p}}{2}\right)$ and so the theorem holds.

B. ELLIPTIC FUNCTIONS AND ELLIPTIC CURVES

6. Elliptic Functions

Definition (Def. I. 6.1)

Let L be any lattice in $\mathbb{C}$.

An elliptic function with periods in L , is by definition, a meromorphic function on $\mathbb{C}$ invariant under translation by the elements of L, and therefore it can be equivalently regarded, as a meromorphic function defined on the torus $\mathbb{C}/_{L}$, which is a compact Riemann surface of genus 1.

Let f be an elliptic function with periods in a lattice L in $\mathbb{C}$, and holomorphic on $\mathbb{C}$. Then, by the above definition, the function f can be regarded as a holomorphic function on the torus $\mathbb{C}/_{L}$. Thus, the function f is bounded, and so by Liouville's theorem must be constant. So, we have proved that:

Theorem (Th. I. 6.2)

Every holomorphic elliptic function is constant.

We can also prove (by integrating f'/f and zf'/f around a fundamental parallelogram) that:

Theorem (Th. I. 6.3)

Let f be an elliptic function defined on the torus $\mathbb{C}/_{L}$. Then, we have:

(i) The number of zeros of f is equal to the number of poles of f, taking the multiplicities into account.

(ii) The sum of zeros of f is equal to the sum of poles of f, taking the multiplicities into account.

The most important examples of elliptic functions are the

$\wp$-Weierstrass function and its derivative $\wp'$. These in fact generate the field of elliptic functions with periods in L over $\mathbb{C}$.

These functions are defined as follows:

$$\wp(z;L) = \frac{1}{z^2} + \sum_{\substack{\omega\in L \\ \omega\neq 0}} \left\{ \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right\} \quad , \qquad \text{(I. 6.4)}$$

$$\wp'(z;L) = -2 \sum_{\omega\in L} \frac{1}{(z-\omega)^3} \qquad \text{(I. 6.5)}$$

It is straight forward to prove the following:

Remark (Rem. I. 6.6)

From (I. 6.2) we deduce $\wp(\lambda z;\lambda L) = \lambda^{-2}\wp(z;L) \quad \forall \lambda\in\mathbb{C}^\times$ Therefore $\wp(-z;L) = \wp(z;L)$, that is, the $\wp$-function is even. From the series expansion (I. 6.4), we deduce that the $\wp$ -function is meromorphic on $\mathbb{C}$, with a double pole at each lattice point, and no other poles.

Also, (I. 6.5) gives $\wp'(\lambda z;\lambda L) = \lambda^{-3}\wp'(z:L) \quad \forall \lambda\in\mathbb{C}^\times$ Therefore $\wp'(-z;L) = -\wp'(z;L)$, that is, the $\wp'$-function is odd. From the series expansion (I. 6.5), we also deduce that the $\wp'$-function is meromorphic on $\mathbb{C}$, with a triple pole at each lattice point, and no other poles.

From (I. 6.5) it is clear that the $\wp'$ -function is invariant under translation by the elements of L. So $\wp'$ is periodic and odd and one proves from that, by integrating that the $\wp$ -function is also elliptic.

From now on we fix the notation :

$L = [\omega_1,\omega_2]$, $\omega_3 = -(\omega_1+\omega_2)$, and $e_i = \wp(\frac{1}{2}\omega_i)$, $i=1,2,3$.

Remark (Rem. I. 6.7)

By (Th. I. 6.3), the $\wp'$-function has three zeros modL with sum $\equiv 0$ (modL). Now, since $\wp'$ is odd, it is clear that these three zeros are at $\frac{1}{2}\omega_1$, $\frac{1}{2}\omega_2$, $\frac{1}{2}\omega_3$ (modL).

Remark (Rem. I. 6.8)

The Weierstrass $\wp$, $\wp'$ functions can be expressed, as Laurent series near the origin, in terms of the Eisenstein series $G_n(L) = \sum_{\substack{\omega \in L \\ \omega \neq 0}} \frac{1}{\omega^{2n}}$.

These expansions are given as follows (Lang [28], p.p. 10-11)

$$\wp(z;L) = \frac{1}{z^2} + \sum_{k \geq 1}^{\infty} (2k+1) G_{k+1}(L) z^{2k} \quad \text{and} \qquad \text{(I. 6.9)}$$

$$\wp'(z;L) = -\frac{2}{z^3} + \sum_{k \geq 1}^{\infty} 2k(2k+1) G_{k+1}(L) z^{2k-1} \qquad \text{(I. 6.10)}$$

Now, set $\phi(z;L) = \wp'(z;L)^2 - (4\wp(z;L)^3 - g_2(L)\wp(z;L) - g_3(L))$ where, $g_2(L) = 60\, G_2(L)$, $g_3(L) = 140\, G_3(L)$. Note, that since $\phi(z;L)$ is a rational function of $\wp$ and $\wp'$, it is an elliptic function with respect to L.

Now, using the Laurent expansions (I. 6.9) and (I. 6.10) it is easy to see that $\phi(z;L)$ has no poles in $\mathbb{C}$ and also that $\phi(0) = 0$. Therefore, by the (Th. I. 6.2), the function $\phi(z;L)$ is identically the zero function. Thus we have proved the following theorem.

Theorem (Th. I. 6.11)

The Weierstrass $\wp$ -function satisfies the following differential equation: $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$.

Now put $\phi_i(z) = \wp(z) - e_i$, (i = 1, 2, 3).

Note, that the function $\phi_i(z)$ is elliptic with a double pole $\equiv 0 \pmod{L}$. So, by the (Th. I. 6.3), the function $\phi_i(z)$ has exactly two zeros (modL) counting the multiplicity.

Note that $\phi_i(\frac{1}{2}\omega_i) = 0$, and since $\phi'(\frac{1}{2}\omega_i) = 0$ we deduce that $\frac{1}{2}\omega_i$ is a double zero of $\phi_i(z)$ modL, and that $\phi_i(z)$ has no other zeros modL.

Therefore, e_1, e_2, e_3 are distinct and the product : $\prod_{i=1}^{3} (\wp(z) - e_i)$

has the same zeros and poles as $\wp'(z)^2$.

So, by (Th. I. 6.11),

$$4\wp(z)^3 - g_2\wp(z) - g_3 = 4\prod_{i=1}^{3}\{\wp(z)-e_i\}$$

Thus, we have proved the following theorem:

Theorem (Th. I. 6.12)

We have:

$$4\wp(z)^3 - g_2\wp(z) - g_3 = 4\left[\wp(z)-e_1\right]\left[\wp(z)-e_2\right]\left[\wp(z)-e_3\right]$$

and furthermore the roots e_i are distinct.

Remark (Re. I. 6.13)

Since the discriminant of the polynomial $4t^3 - g_2 t - g_3$ is actually $\frac{1}{16}\Delta(L)$, where $\Delta(L) = g_2^3(L) - 27 g_3^2(L)$ from the above theorem we deduce that

$$\Delta(L) \neq 0$$

which is a fact already proved in (I. 4.2.3), in a different way.

Now let c be any complex number. The function $\phi(z) = \wp(z)-c$ is elliptic with a double pole at the point 0 of $\mathbb{C}/L$. Therefore, by the (Th. I. 6.3), it has also two zeros u, -u say, lying in $\mathbb{C}/L$

So, we have proved that:

Lemma (Lem. I. 6.14)

The map $\wp : \mathbb{C}/L \setminus \{0\} \longrightarrow \mathbb{C}$ is surjective.

In fact, for any complex number c the equation

$$\wp(z) = c$$

has only two zeros $\pm u \pmod{L}$, $\not\equiv 0 \pmod{L}$.

Finally, we prove the addition theorem of elliptic functions which states as follows:

The Addition Theorem (Th. I. 6.17)

Let $u_1, u_2 \in \mathbb{C}$, $u_1 \neq \pm u_2 \pmod{L}$, and $u_1, u_2, 2u_1+u_2, 2u_2+u_1 \neq 0 \pmod{L}$

Then we have:

$$\wp(u_1+u_2) = -\wp(u_1) - \wp(u_2) + \frac{1}{4}\left\{\frac{\wp'(u_1)-\wp'(u_2)}{\wp(u_1)-\wp(u_2)}\right\}$$

Proof

By the hypothesis, and (Lem. I. 6.14), $\wp(u_1) - \wp(u_2)$ is a non-zero complex number.

Set $a = \frac{\wp'(u_2) - \wp'(u_1)}{\wp(u_2) - \wp(u_1)}$ and $b = \wp'(u_1) - a\,\wp(u_1)$

and thus:

$$\wp'(u_1) = a\,\wp(u_1) + b, \qquad \wp'(u_2) = a\,\wp(u_2) + b$$

The function $\wp'(z) - (a\,\wp(z) + b)$ has a triple pole at 0 of $\mathbb{C}/L$, and hence it has three zeros, counting multiplicities, and two of these are u_1 and u_2, each of multiplicity one. Let u_3 be the third zero, then by the (Th. I. 6.3), we have:

$$u_1 + u_2 + u_3 = 0 \text{ in } \mathbb{C}/L$$

Also: $\wp'(u_3) = a\,\wp(u_3) + b$.

By (Th. I. 6.11), $\wp(u_1)$, $\wp(u_2)$, $\wp(u_3)$ are the roots of the cubic equation

$$4x^3 - g_2 x - g_3 - (ax + b)^2 = 0$$

and therefore $\wp(u_1) + \wp(u_2) + \wp(u_3) = \frac{a^2}{4}$ (1)

Now, substituiting a by $\frac{\wp'(u_2) - \wp'(u_1)}{\wp(u_2) - \wp(u_1)}$ and u_3 by $-(u_1 + u_2)$, in (1), we have the desired formula.

7. Elliptic Curves

7.1 Definitions and General Facts

Definition (Def. I. 7.1.1)

Let K be any field.

An elliptic curve E over K, is said to be, a non-singular projective curve defined over K, of genus 1, which has a point defined over K.

It is known that every elliptic curve over a field K, with Char (K) $\neq 2,3$, is algebraically equivalent over K to a curve given by an equation of the form:

$$Z\,Y^2 = 4\,X^3 - \alpha_2 Z^2 X - \alpha_3 Z^3 \qquad \text{(I. 7.1.2)}$$

where $\alpha_2, \alpha_3 \in K$, and $\alpha_2^3 - 27\alpha_3^2 \neq 0$. Such an equation is said to be in Weierstrass form.

An elliptic curve defined as above has exactly one point at infinity, namely $[(0, 1, 0)] \in P^2(K)$, and setting $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ $(Z \neq 0)$, we obtain in affine form the defining equation of the curve:

$$y^2 = 4x^3 - \alpha_2 x - \alpha_3$$

Note that E is usually regarded as the set of points in $P^2(\bar{K})$ satisfying (I. 7.1.2) with $\bar{K}$ an algebraic closure of K.

The set of K-rational points of E, denoted by E(K), is defined to be the set of points (x, y) of E with $x, y \in K$, together with the point at infinity. It can be shown, by the Reimann-Roch theorem that we can define an abelian (additive) group structure on E, with E(K) being a subgroup, taking the point at infinity as the zero element, which from now on we denote by $\mathcal{O}$.

We are interested in elliptic curves defined over the field of complex numbers, or, over the rationals.

We shall show first, that the parametrization of an elliptic curve, by the Weierstrass $\wp, \wp'$-functions, affords a group structure to the set $E(\mathbb{C})$. Furthermore, we shall investigate the homomorphisms between elliptic curves.

7.2 The Group Structure of the Set of Points of an Elliptic Curve over $\mathbb{C}$.

Using the fact that the absolute invariant j takes every value on the complex plane (Th. I. 4.3.2), one can prove the following:

Lemma (Lem. I. 7.2.1) (Lang [28] p.p. 39, cor. 2)

Given any two complex numbers α_2, α_3 with $\alpha_2^3 - 27\alpha_3^2 \neq 0$,

there exists a lattice $L = [\omega_1, \omega_2]$ with $Im(\frac{\omega_1}{\omega_2}) > 0$

such that: $g_2(\omega_1, \omega_2) = \alpha_2$, $g_3(\omega_1, \omega_2) = \alpha_3$.

Now let E be an elliptic curve with the Weierstrass form $y^2 = 4x^3 - \alpha_2 x - \alpha_3$, where $\alpha_2, \alpha_3 \in \mathbb{C}$ and $\alpha_2^3 - 27\alpha_3^2 \neq 0$.

By the above lemma, we can choose a lattice $L = [\omega_1, \omega_2]$ with $Im(\frac{\omega_1}{\omega_2}) > 0$ such that

$$g_2(L) = \alpha_2 \quad \text{and} \quad g_3(L) = \alpha_3$$

Therefore, by (Th. I. 6.11), we have

$$\wp'(z;L)^2 = 4\wp(z;L)^3 - \alpha_2 \wp(z;L) - \alpha_3 \qquad \text{(I. 7.2.2)}$$

which means that the elliptic curve can always be parametrized by the Weierstrass $\wp, \wp'$ functions.

We, now, take the map

$$f : \mathbb{C}/L \longrightarrow E(\mathbb{C})$$

defined by:

$$f(z) = \begin{cases} (\wp(z), \wp'(z)) & \text{, if } z \neq 0 \\ \mathcal{O} & \text{, if } z = 0 \end{cases} \qquad \text{(I. 7.2.3)}$$

Note that, since both $\wp(z), \wp'(z)$ have poles only at the point 0 of $\mathbb{C}/L$, the map is well-defined.

Note, also, that the map f is bijective.

For, let $(x, y) \in E(\mathbb{C}) \setminus \{\mathcal{O}\}$ Then, by the (Lem I. 6.14), there are only two elements $\pm u \in \mathbb{C}/L \setminus \{0\}$ such that $\wp(u) = x$, and $\wp(-u) = x$.

Now, since (I. 7.2.2), $\wp'(u) = \pm y$, and since $\wp'$ is odd we can find a unique element $V \in \mathbb{C}/L \setminus \{0\}$, such that $V \xmapsto{f} (x, y)$ as follows: If $\wp'(u) = y$, then $V = u$, and if $\wp'(u) = -y$, then $V = -u$. This proves our claim.

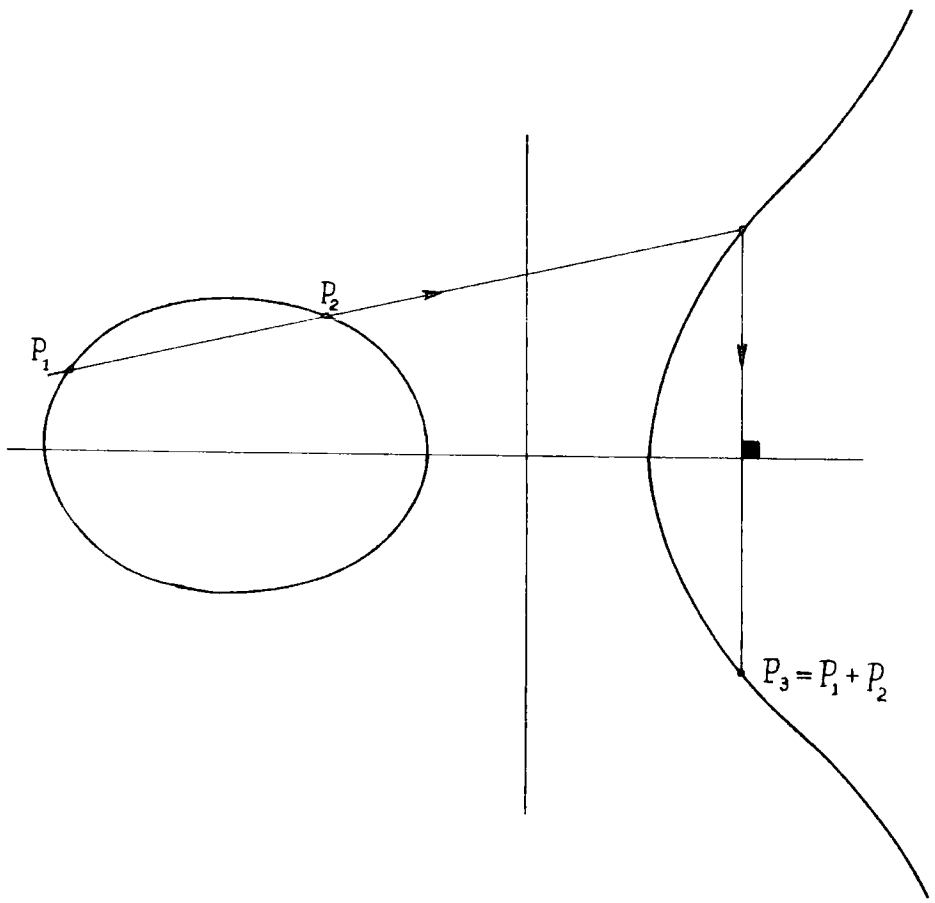
Note, that, since the map f is bijective, the group structure on $\mathbb{C}/L$ induces, via f, a group structure on the set $E(\mathbb{C})$, and from

the addition theorem (Th. I. 6.17) we see that E ($\mathcal{C}$) is an algebraic group with this structure:

If $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ are two points of $E(\mathcal{C})$, then $P_1 + P_2 = P_3$, where $P_3 = (x_3, y_3)$ and

$$x_3 = -x_1 - x_2 + \frac{1}{4}\left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2$$

$$y_3 = -\frac{y_1 - y_2}{x_1 - x_2}\left(x_1 + x_2\right) + \frac{y_2 x_1 - y_1 x_2}{x_2 - x_1}$$



7.3 Homomorphisms on Elliptic Curves

By the previous paragraph, if E, E′ are two elliptic curves isomorphic to $\mathbb{C}/L$, $\mathbb{C}/L'$ respectively then

$$\text{Hom}\ (E, E') \cong \text{Hom}\ (\mathbb{C}/L\ ,\ \mathbb{C}/L')$$

It is easy to prove that:

Lemma (Lem. I.7.3.1) (See Lang [28] , p.p. 14-15, th. 6)

(i) If $\lambda: \mathbb{C}/L \longrightarrow \mathbb{C}/L'$ is a complex analytic homomorphism, then there exists a complex number a such that

$$\lambda(z) \equiv az \ (\text{mod}\, L') \quad \text{and} \quad aL \subseteq L'$$

(ii) If $a \in \mathbb{C}$, and $aL \subseteq L'$, then the map

$$\lambda: \mathbb{C}/L \longrightarrow \mathbb{C}/L' \quad \text{given by} \quad \lambda(z) \equiv az \ (\text{mod}\, L')$$

is a complex analytic homomorphism.

From this lemma, we deduce that:

Theorem (Th. I. 7.3.2)

Let E, and E be elliptic curves isomorphic to $\mathbb{C}/L$, and $\mathbb{C}/L'$ respectively. Then we have:

$$\text{Hom}\ (E, E') \cong \left\{ a \in \mathbb{C} \ :\ aL \subseteq L' \right\} \qquad \text{(I. 7.3.3)}$$

$$\text{End}\ (E) \cong \left\{ a \in \mathbb{C} \ :\ aL \subseteq L \right\} \qquad \text{(I. 7.3.4)}$$

$$\text{Aut}\ (E) \cong \left\{ a \in \mathbb{C} \ :\ aL = L \right\} \qquad \text{(I. 7.3.5)}$$

Note also that:

The curves E, E are isomorphic, as complex analytic manifolds, if and only if, there exists an $a \in \mathbb{C}$ such that $aL = L'$. By the homogeneity of the lattice function j, we deduce that the class of elliptic curves isomorphic to E is determined by $j(L)$, which is the so called, the j-invariant of the curve.

Definition (Def. I. 7.3.6)

Let E be an elliptic curve isomorphic to $\mathbb{C}/L$.

We say that E has a complex multiplication, if there is a non

rational integer $a \in \mathbb{C}$ such that $aL \subseteq L$.

So if E has no complex multiplication, we have:

$$\text{End}(E) \cong \mathbb{Z} \quad , \quad \text{Aut}(E) \cong \{\pm 1\}$$

For the case where E has a complex multiplication, one easily establishes that:

Theorem: (Th. I. 7.3.7)

Let E be an elliptic curve isomorphic to $\mathbb{C}/L$, with complex multiplication by $\alpha \in \mathbb{C} \setminus \mathbb{Z}$.

Set $K = \mathbb{Q}(\alpha)$, $R_0 = \text{int}(K)$, $R(L) = \{\lambda \in K : \lambda L \subseteq L\}$.

We have:

(i) α is an imaginary quadratic algebraic integer.

(ii) $\text{End}(E) \cong R(L)$

(iii) $R(L)$ is a subring of R_0, and

(iv) $\text{Aut}(E) \cong R_0^{\times}$

Note that, since K is an imaginary quadratic field, $R_0^{\times} = \{\pm 1\}$ apart from the cases where K is either $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$.

Therefore there are only two cases in which $R_0^{\times}$ contains more than ± 1 and these are:

Case 1 $K = \mathbb{Q}(\sqrt{-1})$

We have $R_0 = \mathbb{Z}[\sqrt{-1}]$, $R_0^{\times} = \{\pm 1, \pm \sqrt{-1}\}$, and $R(L) = R_0$

Therefore: $\text{End}(E) \cong \mathbb{Z}[\sqrt{-1}]$, and

$\text{Aut}(E) \cong \{\pm 1, \pm \sqrt{-1}\}$

Case 2 $K = \mathbb{Q}(\sqrt{-3})$

We have $R_0 = \mathbb{Z}[\sqrt{-3}]$, $R_0^{\times} = \{\pm 1, \pm \rho, \pm \rho^2\}$ where $\rho = e^{2\pi i/3}$, and $R(L) = R_0$.

Therefore: $\text{End}(E) \cong \mathbb{Z}[\sqrt{-3}]$, and

$\text{Aut}(E) \cong \{\pm 1, \pm \rho, \pm \rho^2\}$

In fact we can tell whether an elliptic curve falls into either

these two cases by looking at its equation in Weierstrass form.

For, let $E : y^2 = 4x^3 - \alpha_2 x - \alpha_3$ be an elliptic curve isomorphic to $\mathbb{C}/L$ with a complex multiplication.

Note that:

$$j_E = 1728, \text{ if and only if, } \alpha_3 = 0$$

In this case, Aut (E) contains at least 4 elements, namely:

$(x, y) \longmapsto (x, \pm y)$, $(x, y) \longmapsto (-x, \pm \sqrt{-1}\, y)$

Also note that:

$$j_E = 0, \text{ if and only if, } \alpha_2 = 0$$

In this case, Aut (E) contains at least 6 elements, namely:

$(x, y) \longmapsto (p^\nu x, \pm y)$, $\nu = 0, 1, 2$, with $p = e^{2\pi i/3}$.

Therefore E belongs to the case 1 (resp. 2), if and only if, $\alpha_2 = 0$ (resp. $\alpha_3 = 0$).

The above results are summarised in the following remark.

Remark (Rem. I. 7.3.8)

Every elliptic curve E over $\mathbb{C}$ belongs to one of the following three classes :

The Class $\mathcal{E}_2$

It contains all elliptic curves with Weierstrass form

$$E : y^2 = 4x^3 - \alpha_2 x$$

where $\alpha_2 \neq 0$.

Furthermore, they have complex multiplication, and

$$\text{End}(E) \cong \mathbb{Z}[\sqrt{-1}]$$

$$\text{Aut}(E) \cong \{\pm 1, \pm \sqrt{-1}\}$$

The Class $\mathcal{E}_3$

It contains all elliptic curves with Weierstrass form

$$E : y^2 = 4x^3 - \alpha_3$$

where $\alpha_3 \neq 0$.

Furthermore, they have complex multiplication, and

$$\text{End}(E) \cong \mathbb{Z}[\sqrt{-3}]$$

$$\text{Aut}(E) \cong \{\pm 1, \pm p, \pm p^2\}$$

where $p = e^{2\pi i/3}$

The Class $\mathcal{E}$

It contains all elliptic curves with Weierstras form

$$E : y^2 = 4x^3 - \alpha_2 x - \alpha_3$$

where $\alpha_2\alpha_3 \neq 0$, and $\alpha_2^3 - 27\alpha_3^2 \neq 0$

Furthermore,

$$\text{Aut}(E) \cong \{ \pm 1 \}$$

7.4 Points of Finite Order of an Elliptic Curve

Let K be any field with Char $(K) \neq 2, 3$, and E an elliptic curve over K.

For any positive integer n, the map

$$E \longrightarrow E$$

given by: $p \longmapsto nP$

is clearly a group homomorphism.

The kernel of this map, that is,

$$E_n = \{ P \in E : nP = \mathcal{O} \}$$

is called the group of n-division points of E.

If the elliptic curve E is defined over $\mathbb{C}$, then in view of the isomorphism $E(\mathbb{C}) \cong \mathbb{C}/L$, it is obvious that

$$E_n(\mathbb{C}) \cong \mathbb{Z}_n \times \mathbb{Z}_n$$

and therefore, there are exactly n^2 elements of order dividing n in $E(\mathbb{C})$.

In general, if the elliptic curve E is defined over an arbitrary field K of characteristic p (p is a prime or 0), then, it can be proved that

$$E_n = \begin{cases} \mathbb{Z}_n \times \mathbb{Z}_n & , \text{ if } p \nmid n \\ \text{subgroup of } \mathbb{Z}_n \times \mathbb{Z}_n, & \text{otherwise.} \end{cases}$$

7.5 Elliptic Curves over a Number Field - The Mordell-Weil Theorem

It is easy to prove that every elliptic curve E defined over $\mathbb{Q}$ is algebraically equivalent over $\mathbb{Q}$ to a curve given by the equation

$$y^2 = x^3 - Ax - B \qquad (1)$$

where A, B are rational integers, and $4A^3 - 27B^2 \neq 0$).
The discriminant of the polynomial $x^3 - Ax - B$, that is ,
$\Delta = 16\,(4A^3 - 27B^2)$, is called the discriminant of E.

In 1922 L.J. Mordell proved that E ($\mathbb{Q}$) is a finitely generated abelian group, and this was conjectured by H. Poincaré in 1901. In 1928 A. Weil extended this result to an arbitrary algebraic number field. We state this remarkable result, which is referred to as the Mordell-Weil theorem.

The Mordell-Weil Theorem (Th. I. 7.5.1) (See Lang [29] , p.p. 84, § 2)

If E is an elliptic curve defined over a number field K, then E (K) is a finitely generated abelian group.

CHAPTER II

THE APPLICATION OF MODULAR FUNCTIONS INTO THE CLASS FIELD THEORY OF IMAGINARY QUADRATIC FIELDS

1. Standard Notations and General Facts

In the following, we denote by p a prime rational integer, and by ω an imaginary quadratic surd so that:

$$A\omega^2 + B\omega + C = 0 \quad , \qquad (1)$$

where A, B, C, are relatively prime integers such that

$$A > 0 > B^2 - 4AC.$$

We set $K = \mathbb{Q}(\omega)$, and denote by:

R, any order in K

R_0 , the maximal order in K, that is $R_0 = \text{int}(K)$

D, the discriminant of R_0 . We have:

(i) $D \equiv 0$ or $1 \pmod 4$, and D is not a square.

(ii) D determines the quadratic field K, and thus we may write $h(D)$ for the class number of the field K.

(iii) The Dirichlet class number formula (see Markus [31] p.p. 201-202, th. 46):

$$h(D) = \frac{1}{2-\left(\frac{D}{2}\right)} \left| \sum_{\substack{(k,D)=1 \\ 0<k<\frac{|D|}{2}}} \left(\frac{D}{k}\right) \right| \quad , \text{ if } D<-4 \qquad \text{(II. 1.1)}$$

where $\left(\frac{D}{k}\right)$, is the Kronecker symbol.

$\mathfrak{D}$, the absolute value of the discriminant of R_0 , that is

$$\mathfrak{D} = |\text{disc}(R_0)| \ .$$

$\mathfrak{D}(\omega)$, the absolute value of the discriminant of (1), that is

$$\mathfrak{D}(\omega) = |B^2 - 4AC| \ .$$

Λ , the lattice $\langle \omega, 1 \rangle$.

$R(\Lambda)$, the order of the lattice Λ, which by definition, is,

$$R(\Lambda) = \{ \lambda \in \mathbb{C} : \lambda\Lambda \subseteq \Lambda \}$$

Note, that since $-\mathfrak{D}(\omega) = B^2 - 4AC$, $B \equiv -\mathfrak{D}(\omega) \pmod 2$, and hence:

$$\left\langle \frac{-\mathfrak{D}(\omega) + \sqrt{-\mathfrak{D}(\omega)}}{2} , 1 \right\rangle = \left\langle \frac{B + \sqrt{-\mathfrak{D}(\omega)}}{2} , 1 \right\rangle$$

It is easly seen, that:

$$R(\Lambda) = \left\langle \frac{-\mathfrak{D}(\omega) + \sqrt{-\mathfrak{D}(\omega)}}{2} , 1 \right\rangle = \left\langle \frac{B + \sqrt{-\mathfrak{D}(\omega)}}{2} , 1 \right\rangle$$

We also denote by:

$M(R)$, the conductor of the order R in K, that is, by definition, $M(R) = \left| R_0/R \right|$. It is known that if $R_0 = \mathbb{Z}_{[z]}$ then $R = \mathbb{Z}_{[M(R)z]}$

It is also easily verified that the conductor of the order $R(\Lambda)$, is the unique positive integer M such that $\mathcal{D}(\omega) = M^2\mathcal{D}$, which is also called the conductor of ω . It $M = 1$, we say that ω is primitive;

In this case, of course, $R(\Lambda) = R_0$, and if $\omega \in R_0$ then $R_0 = \mathbb{Z}_{[\omega]}$

Now, we denote by:

S, a finite set of rational prime integers.

m , any positive rational integer with prime factors in S.

$I_S(R)$, the multiplicative group containing all fractional ideals of K, prime to S, with respect to the order R, that is the free abelian group generated by all prime ideals of R in K, which are prime to S.

So, we have:

$$I_S(R) \subseteq I_S(R_0) \subseteq I_K \ ,$$

where I_K is the ideal group of K.

$P_{S,m}(R)$, the multiplicative group containing all principal fractional ideals of K, prime to S, of the form $(n + m\alpha)_R$, where $n \in \mathbb{Z}$, and $\alpha \in R$.

So, we have:

$$P_{S,m}(R) \subseteq P_K \ ,$$

where P_K is the principal ideal group of K, and that for any positive integer m having prime factors in S.

$P_{S,1,m}(R)$, the subgroup of $P_{S,m}(R)$ containing all principal fractional ideals of K, prime to S, of the form $(1 + m\alpha)_R$,where $\alpha \in R$.

Now, we state some results of the class-field theory on imaginary quadratic fields (quoted from [4],[15] and [44]).

2. General Results

Theorem (Th. II. 2.1)

To any subgroup H, such that

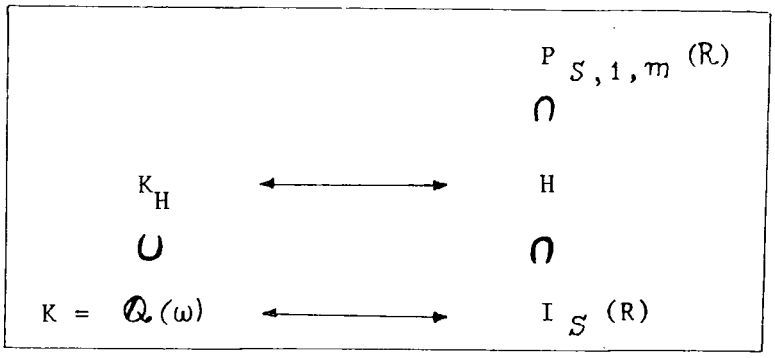
$$I_S(R) \supseteq H \supseteq P_{S,1,m}(R)$$

for some positive integer m with prime factors in S, there is a unique abelian extension K_H of $K = \mathbb{Q}(\omega)$ with the following properties:

(i) The K_H/K norms of integral ideals in K_H prime to S are in H.

(ii) K_H is unramified outside S, and

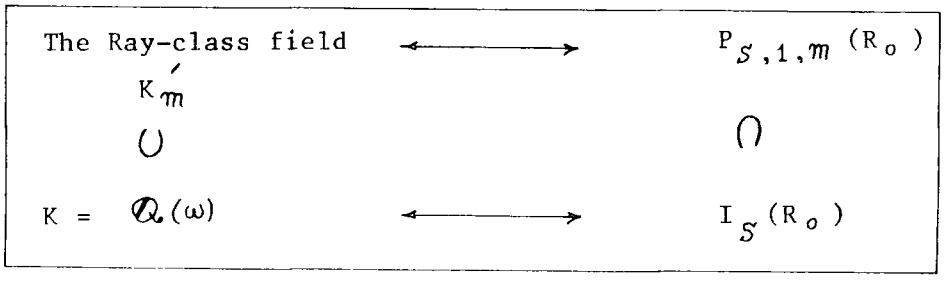
(iii) $\mathrm{Gal}(K_H : K) \cong I_S(R)/H$.



In particular we have:

(i) To $P_{S,1,m}(R_o)$ corresponds the Ray-class field modulo m (denoted K'_m), and so

$$\mathrm{Gal}(K'_m : K) \cong I_S(R_o)/P_{S,1,m}(R_o)$$

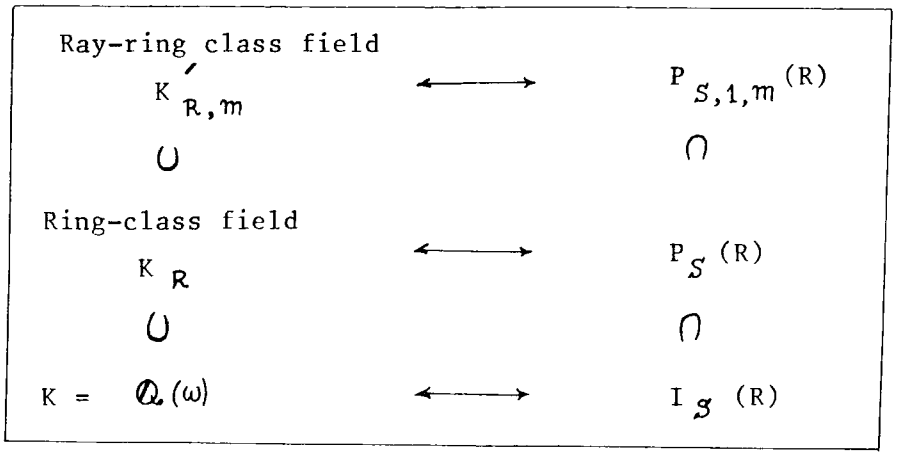


(ii) Let m be any positive integer with prime factors in S. To the subgroups $P_S(R)$, $P_{S,1,m}(R)$ with

$$I_S(R) \supset P_S(R) \supset P_{S,1,m}(R)$$

correspond, respectively, the fields K_R , $K'_{R,m}$, namely the Ring-class field with respect to R , the Ray-ring class field with

respect to R and $\mathfrak{m}$, respectively.

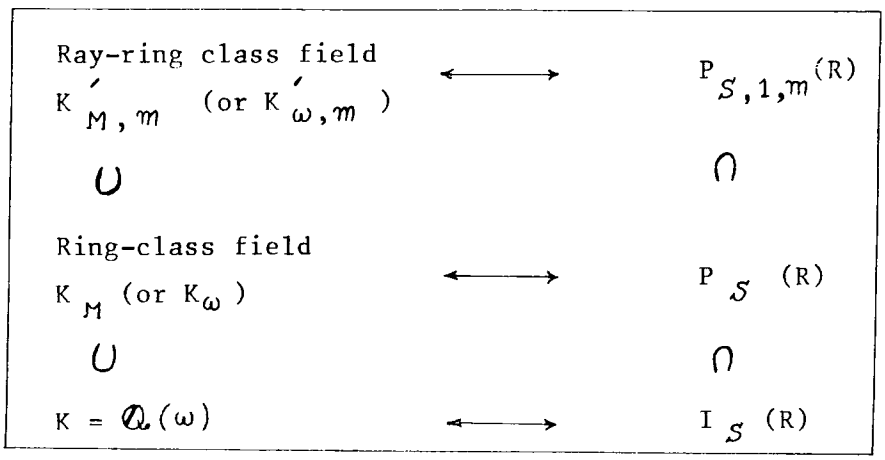


(iia) If $R = R(\Lambda)$, since

$$\text{cond}(\omega) = \text{cond}(R) = M,$$

we may replace the symbol R by M (or by ω), in the above class field correspondence.

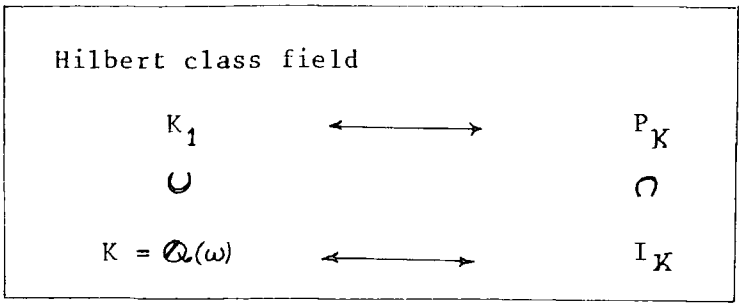
So we have:



In this case, we may call, K_M (resp. K_ω) the ring-class field modulo M (resp. the ring-class field with respect to ω), and $K'_{M,\mathfrak{m}}$ (resp. $K'_{\omega,\mathfrak{m}}$) the ray-ring class field with respect to M and $\mathfrak{m}$ (resp. the ray-ring class field with respect to ω and $\mathfrak{m}$), of $K = \mathbb{Q}(\omega)$.

The ring-class field K_1, that is K_ω with $\text{cond}(\omega) = 1$, is called the Hilbert class field or the absolute class field, of $K = \mathbb{Q}(\omega)$.

In this case the class field correspondence is as follows:



In this case, of course, $\mathrm{Gal}(K_1 : K) \cong I_K / P_K = C_K$, and the degree of the extension $K_1 : K$ is the class number h_k of $K = \mathbb{Q}(\omega)$. We have also, that K_1 is the unique abelian maximal unramified extension of $K = \mathbb{Q}(\omega)$ and corresponds to the group of principal ideals.

Theorem (Th. II. 2.2) (see Lang [28], p.p. 133, Th. 5)

If ω has conduction M then $j(\omega)$ generates the ring-class field modulo M of $K = \mathbb{Q}(\omega)$ over $\mathbb{Q}(\omega)$, that is, $K_\omega = \mathbb{Q}(\omega, j(\omega))$.

Theorem (Th. II. 2.3) (see Lang [28], p.p. 95, Th. 7)

Let K be any imaginary quadratic field, and R be any order in K with conductor M. Then we have:

$$\left[K_M : K\right] = h_K \frac{M}{(R_o^\times : R^\times)} \prod_{p|M} \left(1 - \left(\frac{K}{p}\right) \frac{1}{p}\right)$$

where $R_o^\times$, and $R^\times$ are the group units in R_o, and R, respectively, and $\left(\frac{K}{p}\right)$ is given by:

$$\left(\frac{K}{p}\right) = \begin{cases} 0 & \text{if p ramifies in K} \\ 1 & \text{if p splits completely in K} \\ -1 & \text{if p remains prime} \end{cases}$$

Furthermore, by the tower $K_M \supset K_1 \supset K$ we have:

$$\left[K_M : K_1\right] = \frac{M}{(R_o^\times : R^\times)} \prod_{p|M} \left(1 - \left(\frac{K}{p}\right) \frac{1}{p}\right) .$$

3. The Söhngen Theorem

We state, now, a very important result due to H. Söhngen (see Söhngen [44], also Shimura [40], p.p. 140, pr. 6.9)

Söhngen's Theorem (Th. II 3.1)

Suppose that $f(\tau)$ is a modular function of weight 0, for $\hat{\Gamma}(N)$ and the Fourier expansions of $f(\tau)$ at every cusp of $\hat{\Gamma}(N)$ for $\mathfrak{H}^*$ have coefficients in the cyclotomic field $\mathbb{Q}(e^{2\pi i/N})$.

If ω has conductor M, then $f(\omega)$ is in the class field corresponding to the group H generated by principal ideals of the form:

$$\prec 1 + N\alpha + NM\beta \succ_R$$

with $\alpha \in \mathbb{Z}$, and $\beta \in R$.

In particular, $f(\omega)$ lies inthe ray-class field modulo M N, K'_{MN}, and furthermore $f(\omega)$ generates an abelian extension of $\mathbb{Q}(\omega)$.

4. The Case, where $D = -p$, $p \equiv 3 \pmod 4$, and $p > 3$

Let $K = \mathbb{Q}(\sqrt{-p})$, and $R_o = \text{int}(K)$.

We have: $R_o = \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$, and $R_o^\times = \{\pm 1\}$.

Now, if R is any order in K with conductor M then $R^\times = \{\pm 1\}$, and by the (Th. II. 2.3),

$$\left[K_M : K_1\right] = M \prod_{p|M} \left(1 - \left(\frac{K}{p}\right)\frac{1}{p}\right) . \qquad \text{(II. 4.1)}$$

Theorem (Th. II. 4.2)

The class-number $h(-p)$ is odd.

Proof

Since p is odd, the Kronecker symbol $\left(\frac{-p}{k}\right)$ mentioned in the class number formula (II. 1.1) is actually the Legendre symbol $\left(\frac{k}{p}\right)$.

We also know that:

$$\left(\frac{2}{p}\right) = \begin{cases} -1 & , \text{ if } p \equiv 3 \pmod 8 \\ 1 & , \text{ if } p \equiv 7 \pmod 8 \end{cases}$$

Therefore, the class number formula can be written as:

$$h(-p) = \begin{cases} \frac{1}{3}\left|\sum_{k=1}^{\frac{p-1}{2}}\left(\frac{k}{p}\right)\right|, & \text{if } p \equiv 3 \pmod 8 \\ \left|\sum_{k=1}^{\frac{p-1}{2}}\left(\frac{k}{p}\right)\right|, & \text{if } p \equiv 7 \pmod 8 \end{cases} \qquad \text{(II. 4.3)}$$

Note that, since $p \equiv 3 \pmod 4$, $\frac{p-1}{2}$ is odd.

Hence, in the sum $\sum_{k=1}^{\frac{p-1}{2}}\left(\frac{k}{p}\right)$ appear an odd number of ± 1, and so, the whole sum is an odd number. Therefore, from (II. 4.2), we deduce that $h(-p)$ is odd.

From algebraic number theory we pick the following classical proposition, which is easy to prove.

Lemma (Lem. II. 4.4)

Let $\mathbb{Q}(\sqrt{d})$ be a quadratic field, where d is a square-free rational integer, and q be a prime rational integer. Then we have:

(i) If $q \nmid d$, and q is odd, then

$$\prec q \succ = \begin{cases} \prec q, n + \sqrt{d} \succ \prec q, n - \sqrt{d} \succ & \text{, if } d \equiv n^2 \pmod q. \\ \text{prime, if d is a non (qr) mod q .} \end{cases}$$

(ii) If $q = 2$, and $2 \nmid d$, then

$$\prec 2 \succ = \begin{cases} \prec 2, \ 1 + \sqrt{d} \succ^2, & \text{if } d \equiv 3 \pmod 4 \\ \prec 2, \ \frac{1+\sqrt{d}}{2} \succ \prec 2, \ \frac{1-\sqrt{d}}{2} \succ, & \text{if } d \equiv 1 \pmod 8 \\ \text{prime, if } d \equiv 5 \pmod 8 \end{cases}$$

(iii) If $q \mid d$ then $\prec q \succ = \prec q, \sqrt{d} \succ^2$, where $\prec q, \sqrt{d} \succ$ is a prime ideal.

Theorem (Th. II. 4.5)

We have: $$\left[K_2 : K_1\right] = \begin{cases} 3 & \text{, if } p \equiv 3 \pmod 8 \\ 1 & \text{, if } p \equiv 7 \pmod 8 \end{cases}$$

and $K_2' = K_2$

Proof

By the above lemma, setting $K = \mathbb{Q}(\sqrt{-p})$, and $q = 2$ we have:

If $p \equiv 3 \pmod 8$, then $-p \equiv 5 \pmod 8$, and therefore 2 remains prime in K. Hence $\left(\frac{K}{2}\right) = -1$.

If $p \equiv 7 \pmod 8$, then $-p \equiv 1 \pmod 8$, and therefore 2 splits completely in K. In fact,

$$< 2 > = < 2, \frac{1 + \sqrt{-p}}{2} >< 2, \frac{1 - \sqrt{-p}}{2} >$$

Hence $\left(\frac{K}{2}\right) = 1$.

Therefore, by (II. 4.1), we have:

$$\left[K_2 : K_1\right] = 2\left(1 - \left(\frac{K}{2}\right)\frac{1}{2}\right) = \begin{cases} 3, & \text{if } p \equiv 3 \pmod 8 \\ 1, & \text{if } p \equiv 7 \pmod 8 \end{cases}$$

Also $K_2' = K_2$, since the corresponding ideal groups are clearly the same.

Theorem (Th. II. 4.6)

We have: $\left[K_3 : K_1\right] = \begin{cases} 2, & \text{if } p \equiv 2 \pmod 3 \\ 4, & \text{if } p \equiv 1 \pmod 3 \end{cases}$

and $K_3' = K_3$.

Proof

By the above lemma, setting $q = 3$, we have:

If $p \equiv 2 \pmod 3$, then $-p \equiv 1 \pmod 3$, and therefore 3 splits completely in K. In fact

$$< 3 > = < 3, 1 + \sqrt{-p} >< 3, 1 - \sqrt{-p} >$$

Therefore $\left(\frac{K}{3}\right) = 1$.

If $p \equiv 1 \pmod 3$, then $-p \equiv 2 \pmod 3$, and therefore 3 remains prime in K. Therefore $\left(\frac{K}{3}\right) = -1$

Hence, by (II. 4.1), we have:

$$\left[K_3 : K_1\right] = 3\left(1 - \left(\frac{K}{3}\right)\frac{1}{3}\right) = \begin{cases} 2, & \text{if } p \equiv 2 \pmod 3 \\ 4, & \text{if } p \equiv 1 \pmod 3 \end{cases}$$

Also $K_3' = K_3$ since the corresponding ideal groups are clearly the same.

CHAPTER III

THE DETERMINATION OF ALL IMAGINARY QUADTRATIC FIELDS WITH CLASS NUMBER ONE

1. The 10th Gauss Discriminant Problem

Let K be any imaginary quadratic field, R_o = int (K), and disc (R_o) = -p, where p is a positive rational integer.

We denote by h (-p) the class number of the field K. We keep fixed the above notation throughout this chapter.

We now state the main theorem, which was conjectured by Gauss, and is famous as the 10th Gauss Discriminant Problem .

Theorem (Th. III. 1.1)

There are exactly nine imaginary quadratic fields with class number h (-p) = 1, given by

p = 3, 4, 7, 8, 11, 19, 43, 67, 163

We proceed to build up a proof of this theorem, and in this section using elementary algebraic Number Theory we reduce the proof to the consideration of the case $p \equiv 3 \pmod 8$ with p a rational prime integer.

Theorem (Th. III. 1.2)

If K is an imaginary quadratic field with h (-p) = 1, then p = 4 or 7 or 8 or $p \equiv 3 \pmod 8$ and p is a rational prime integer.

Proof

Let $K = \mathbb{Q}(\sqrt{d})$, where d is a square-free negative rational integer. Suppose that $d \not\equiv 1 \pmod 4$, then -p = 4d, and $R_o = \mathbb{Z}\left[\frac{\sqrt{-p}}{2}\right]$. By (Lem II. 4.4), and since h (-p) = 1, we have $\langle 2 \rangle = \langle x + y \frac{\sqrt{-p}}{2} \rangle^2$ for some rational integers x, y. Taking norms on both sides we have: $4 = \left(x^2 + \frac{p}{4} y^2\right)^2$ (1). It is easy to check that (1) has integral solution, if and only if, p = 4 or p = 8.

Hence, the only possible cases are:

p = 4, or p = 8, or $p \equiv 3 \pmod 4$.

Suppose now that $p \equiv 3 \pmod 4$. Then $-p = d$, and $R_o = \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$

Let us start with the case where $p \equiv 7 \pmod 8$.

By (Lem. II. 4.4), we have:

$$\langle 2 \rangle = \langle 2, \frac{1+\sqrt{-p}}{2} \rangle \langle 2, \frac{1-\sqrt{-p}}{2} \rangle \qquad (2)$$

Since $h(-p) = 1$, each ideal on the right hand side of (2) is principal. Therefore, there is an element

$$\alpha = \frac{x + y\sqrt{-p}}{2} \in R_o$$

such that $N(\alpha) = 2$, that is, there exist rational integers x, y with $x \equiv y \pmod 2$ such that:

$$\frac{x^2}{4} + p\frac{y^2}{4} = 2 \quad , \text{ that is } x^2 + p y^2 = 8 \qquad (3)$$

Since $p \equiv 7 \pmod 8$, it is easy to check that (3) has integral solution, if and only if, $p = 7$.

So far the only possible cases are :

$$p = 4, \text{ or } p = 8, \text{ or } p = 7, \text{ or } p \equiv 3 \pmod 8$$

and so we have only to prove that, if $p \equiv 3 \pmod 8$, then p is a rational prime.

For, suppose that $p \equiv 3 \pmod 8$, and p is a composite square free. Then there exists an odd prime q, such that $q(q+2) \leq p$, and $q \mid p$.

Since $h(-p) = 1$, there is an element

$$\alpha = \frac{x + y\sqrt{-p}}{2} \in R_o$$

where x, y are rational integers, such that $N(\alpha) = q$, that is $x^2 + p y^2 = 4q$.

But $4q = x^2 + p y^2 \geq p y^2 \geq q(q+2) y^2$,

and so $4 \geq (q+2) y^2$

Since q is odd, $q + 2 \geq 5$, and so $4 \geq 5 y^2$.

Hence $y = 0$, that is $x^2 = 4q$ - contradiction.

So, if $h(-p) = 1$, and $p \equiv 3 \pmod 8$, then p is a rational prime, and hence the theorem holds.

Note, that, the single cases, where p = 4 or 7 or 8 easily lead to h (-p) = 1. Therefore the main interesting poing is to determine among all rational primes $p \equiv 3 \pmod 8$ those having h (-p) =1. For technical reasons, we exclude the case p = 3, where, of course, it is known that h (-p) = 1.

2. The Proof of Gauss' Theorem

From now on, we suppose that

$$h(-p) = 1 \quad ,$$

$p \equiv 3 \pmod 8$, $p > 3$, and p is a rational prime.

We also set:

$$\omega = \frac{1 + \sqrt{-p}}{2}$$

In this case, in view of the results of the § II. 4, we have:

$$K_1 = K = \mathbb{Q}(\sqrt{-p})$$

$$\text{int}\ (K_1 \cap \mathbb{R}) = \mathbb{Z}$$

$$\left[K_2 : K_1\right] = 3,\ K_2' = K_2$$

$$\left[K_3 : K_1\right] = 2 \text{ or } 4,\ K_3' = K_3$$

Also, by the (Th. I. 5.2.12), and since $j(\omega) \in K_1$, we have that, $j(\omega)$ is a rational integer less than zero. Finally, by the (Th. II. 2.2), $K_2 = K_1(j(\sqrt{-p}))$.

2.1 Lemma (Lem. III. 2.1)

$\gamma_2(\omega + 1)$ is a real algebraic integer less than zero, and lies in K_1. Therefore $\gamma_2(\omega + 1)$ is a rational integer less than zero.

Proof

Since $\gamma_2(\tau)$ is invariant under $\overset{\lambda}{\Gamma}(3)$, we have

$$\gamma_2(\omega + 1) = \gamma_2\left(\frac{3 + \sqrt{-p}}{2}\right) = \gamma_2\left(\frac{3 + \sqrt{-p}}{2} - 3\right) = \gamma_2\left(\frac{-3 + \sqrt{-p}}{2}\right)$$

and from (Th. I. 5.2.5), we have that $\gamma_2(\omega + 1)$ is a real algebraic integer less than zero.

Now we prove that $\gamma_2(\omega + 1) \in K_1$.

By (Th. I. 4.5.6), and since $\gamma_2^3(\tau) = j(\tau)$, the function $\gamma_2(\tau)$

has a Fourier expansion at every cusp of $\hat{\Gamma}(3)$ with coefficients in $\mathbb{Q}(e^{2\pi i/3})$. Therefore, by Söhngen's theorem, we have $\gamma_2(\omega+1) \in K_3'$ and so $\gamma_2(\omega+1) \in K_3$.

Now, take the tower of fields

$$K_3 \supset K_1(\gamma_2(\omega+1)) \supset K_1$$

and note that $\gamma_2(\omega+1)$ is the real zero the polynomial

$$x^3 - j(\omega+1)$$

that is,

$$\phi(x) = x^3 - j(\omega) \in \mathbb{Z}[x]$$

Since $\left[K_3 : K_1\right] = 2$ or 4 , we have

$$\left[K_1(\gamma_2(\omega+1)) : K_1\right] = 1 \text{ or } 2$$

And since $\gamma_2(\omega+1)$ is the only real root of $\phi(x)$, $\left[K_1(\gamma_2(\omega+1)) : K_1\right] \neq 2$, and so $\gamma_2(\omega+1)$ lies in K_1 .

Now, since $\text{int}(K_1 \cap \mathbb{R}) = \mathbb{Z}$, $\gamma_2(\omega+1)$ is a negative rational integer as required.

Theorem (Th. III. 2.2)

The equation: $(t-16)^3 = j(\omega)t$ (1) has a unique real root which is also positive. The roots of (1) are $f^{24}(\omega)$, $-f_1^{24}(\omega)$, $-f_2^{24}(\omega)$, and $-f_2^{24}(\omega)$ is the unique real positive root. Furthermore, all of $f^{24}(\omega)$, $-f_1^{24}(\omega)$, $-f_2^{24}(\omega)$ lie in K_2 , and in fact $K_2 = K_1(f_2^{24}(\omega))$.

Proof

We take the polynomial $\phi(t) = (t-16)^3 - j(\omega)\, t \in \mathbb{Z}[t]$

Note that, for real t, $\phi'(t) = 3(t-16)^2 - j(\omega) > 0$, since $j(\omega) < 0$. Therefore $\phi(t)$ has a unique real zero.

Also, since $\phi(0).\phi(16) = 16^4 j(\omega) < 0$, $\phi(t)$ has a real zero lying in (0, 16). So the equation (1) has a unique real root, which is also positive.

By (Th. I. 4.6.9), $f^8(\omega)$, $-f_1^8(\omega)$, $-f_2^8(\omega)$ are the roots

of the equation $x^3 - \gamma_2(\omega)\, x - 16 = 0$, and so clearly the $f^{24}(\omega)$, $-f_1^{24}(\omega)$, $-f_2^{24}(\omega)$ are the roots of the equation (1); among these only one can be real and positive, and from (I. 4.6.1) this is $-f_2^{24}(\omega)$.

From the (Th. I. 4.6.16), we deduce that

$$f^{24}(\omega),\ -f_1^{24}(\omega),\ -f_2^{24}(\omega) \text{ all lie in } K_2' = K_2$$

Now we prove that $f_2^{24}(\omega)$ generates K_2 over K_1.

Because $K_2 = K_1(j(\sqrt{-p})) \supset K_1(f_2^{24}(\omega))$

it is enough to prove that $j(\sqrt{-p}) \in K_1(f_2^{24}(\omega))$

We have already proved in (I. 5.2.9), that

$$f_2\left(\frac{\tau-3}{2}\right) = \frac{\sqrt{2}\, e^{-\pi i/8}}{f(\tau)} \qquad \forall \tau \in \mathfrak{H}$$

Therefore

$$f^{24}(\sqrt{-p}) = \frac{-2^{12}}{f_2^{24}\left(\frac{-3+\sqrt{-p}}{2}\right)} \tag{2}$$

and since $f_2^{24}(\tau)$ is invariant under $\Gamma(2)$,

$$f_2^{24}\left(\frac{-3+\sqrt{-p}}{2}\right) = f_2^{24}\left(\frac{-3+\sqrt{-p}}{2} + 2\right) = f_2^{24}(\omega)$$

So (2) can be written as

$$f^{24}(\sqrt{-p}) = \frac{-2^{12}}{f_2^{24}(\omega)} \tag{3}$$

Now, for every $\tau \in \mathfrak{H}$, $f^{24}(\tau)$ is a root of

$$(t - 16)^3 = j(\tau)\, t$$

and so $$j(\tau) = \frac{(f^{24}(\tau) - 16)^3}{f^{24}(\tau)}$$

Therefore

$$j(\sqrt{-p}) = \frac{(f^{24}(\sqrt{-p}) - 16)^3}{f^{24}(\sqrt{-p})} \tag{4}$$

In view of (3) and (4) we have:

$$j(\sqrt{-p}) = \frac{(2^8 + f_2^{24}(\omega))^3}{(f_2^{24}(\omega))^2}$$

So $j(\sqrt{-p}) \in K_1(f_2^{24}(\omega))$, as required.

2.3 Theorem (Th. III. 2.3.1)

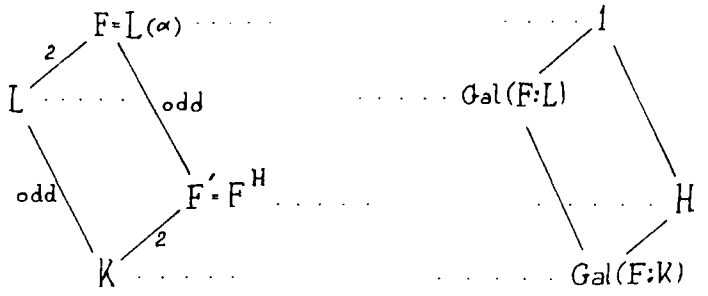
The number $e^{-\pi i/12} f_2^2(\omega)$ is a real algebraic integer, and lies in K_2.

We need a lemma from Galois Theory.

Lemma (Lem. III. 2.3.2)

Let $F \supset L \supset K$ be an abelian tower of fields with $L : K$ of odd degree. Suppose there is an $\alpha \in F$, $\alpha^2 \in L$ and $N_{L/K}(\alpha^2) = \beta^2$, for some $\beta \in K$. Then $\alpha \in L$.

Proof of the Lemma



We may assyme that $F = L(\alpha)$. Suppose for a contradiction that $\mathrm{Gal}(F : L) = \langle \sigma \rangle$, where $\sigma \neq 1_d$, so $\alpha^\sigma = -\alpha$.

Since $\mathrm{Gal}(F : L)$ is of order $2r$ where r is a positive odd number, it has a unique subgroup, H say, of index 2. Let F' be the fixed field corresponding to H.

Note that $$N_{F/F'}(\alpha) = \prod_{h \in H} \alpha^h$$

so $$(N_{F/F'}(\alpha))^\sigma = (-1)^{|H|} \prod_{h \in H} \alpha^h$$

and hence $$(N_{F/F'}(\alpha))^\sigma = - N_{F/F'}(\alpha) \qquad (1)$$

On the other hand, we have

$$-\beta^2 = N_{L/K}(-\alpha^2) = N_{L/K}(N_{F/L}(\alpha)) = N_{F/K}(\alpha)$$
$$= N_{F'/K}(N_{F/F'}(\alpha)) = -(N_{F/F'}(\alpha))^2 .$$

Therefore $N_{F/F'}(\alpha) = \pm \beta$ - contradiction, since by (1), $N_{F/F'}(\alpha)$ is moved by σ, and $\pm \beta$ is not.

So $\sigma = 1_d$, that is $\alpha \in L$.

Proof of the Theorem

In view of the lemma, and (Th. I. 4.6.10), we proceed as follows:

Take $\alpha = -i f_2^{12}(\omega)$, and note that $\alpha^2 = -f_2^{24}(\omega) \in K_2$.

Since α^2 is a root of $(t - 16)^3 = j(\omega)\, t$, we have $N_{K_2/K_1}(\alpha^2) = 2^{12}$

So by the lemma $-i f_2^{12}(\omega) \in K_2$. From (I. 4.6.1), it is easily seen that $-i f_2^{12}(\omega)$ is real and positive, and therefore $N_{K_2/K_1}(-i f_2^{12}(\omega)) = 2^6$. Repeating the lemma again for $\alpha = e^{3\pi i/4} f_2^6(\omega)$ we also have that

$$e^{3\pi i/4} f_2^6(\omega) \in K_2 \qquad (2)$$

Now, note that

$$e^{2\pi i/3} f_2^8(\omega) = \frac{f_2^{24}(\omega) + 16}{e^{-2\pi i/3} \gamma_2(\omega)} = \frac{f_2^{24}(\omega) + 16}{\gamma_2(\omega+1)}$$

By the (Lem III 2.1), $\gamma_2(\omega + 1) \in \mathbb{Z}$.

Also by the (Lem. III. 2.2), $f_2^{24}(\omega) \in K_2$.

Therefore $$e^{2\pi i/3} f_2^8(\omega) \in K_2 \qquad (3)$$

Now, since (2), (3), and

$$\frac{e^{2\pi i/3} f_2^8(\omega)}{e^{3\pi i/4} f_2^6(\omega)} = e^{-\pi i/12} f_2^2(\omega)$$

we have that

$$e^{-\pi i/12} f_2^2(\omega) \in K_2$$

Since (I. 4.6.1), it is easly seen that $e^{-\pi i/12} f_2^2(\omega)$ is real and positive, and by the (Lem III. 2.2) it is also algebraic over K_1 and indeed cubic.

Remark It is now clear that the function which Birch names σ is $e^{-\pi i/24} f_2$ (Cf . Birch [5])

2.4 By the (Th. III. 2.3.1), $V = e^{-\pi i/12} f_2^2(\omega)$ is a root of the equation:

$$x^3 - \kappa x^2 + \lambda x - 2 = 0 \qquad (4)$$

where κ , λ are real algebraic integers lying in K_1 , and so they are rational integers.

Also, note that the roots of (4) are three of the roots of the equation:

$$x^{12} - \gamma_2(\omega+1) x^4 - 16 = 0 \qquad (5)$$

Let ρ_i , $i = 1, 2, 3$ the roots of (4), then

$$\rho_i^4 = \kappa \rho_i^3 - \lambda \rho_i^2 + 2\rho_i \quad , \; i = 1, 2, 3 .$$

So, $$\sum \rho_i^4 = \kappa \sum \rho_i^3 - \lambda \sum \rho_i^2 + 2 \sum \rho_i$$

$$= \kappa (\kappa \sum \rho_i^2 - \lambda \sum \rho_i + 6) - \lambda \sum \rho_i^2 + 2 \sum \rho_i$$

$$= (\kappa^2 - \lambda) \sum \rho_i^2 + (2 - \kappa\lambda) \sum \rho_i + 6\kappa$$

$$= (\kappa^2 - \lambda) \left\{ (\sum \rho_i)^2 - 2 \sum_{i<j} \rho_i \rho_j \right\} + (2 - \kappa\lambda) \sum \rho_i + 6\kappa$$

$$= (\kappa^2 - \lambda)(\kappa^2 - 2\lambda) + (2 - \kappa\lambda)\kappa + 6\kappa$$

$$= \kappa^4 + 8\kappa - 4\kappa^2\lambda + 2\lambda^2$$

By (5), ρ_i^4 , i = 1, 2, 3 are the roots of

$$x^3 - \gamma_2(\omega + 1)\, x - 16 = 0$$

and therefore $$\sum \rho_i^4 = 0$$

So we deduce that

$$\kappa^4 + 8\kappa - 4\kappa^2\lambda + 2\lambda^2 = 0 \qquad (6)$$

From (6) it is easly seen that

$$\kappa \equiv \lambda \equiv 0 \pmod 2$$

and so setting $\kappa = -2\alpha$, and $\lambda = 2\beta$ we deduce from (6) that,

$$\beta^2 - 4\alpha^2\beta + 2\alpha^4 - 2\alpha = 0$$

which can be written as $(\beta - 2\alpha^2)^2 = 2\alpha(\alpha^3 + 1)$

Remark Note that, in fact, V satisfies $V^3 + 2\alpha V^2 + 2\beta V - 2 = 0$ and not $V^3 - \alpha V^2 + \beta V - 2 = 0$ (C.F. Birch [5], Equation (8)).

2.5 The Solution of the Diophantine Equation

$$(\beta - 2\alpha^2)^2 = 2\alpha(\alpha^3 + 1) \qquad (7)$$

Putting $\alpha = -x$, (7) is reduced to

$$(\beta - 2x^2)^2 = 2x(x^3 - 1) \qquad (8)$$

Set $y = \beta - 2x^2$, so (8) is reduced to

$$y^2 = 2x(x^3 - 1) \qquad (9)$$

We find the integral solutions of (9).

The trivial cases, where either x or $x^3 - 1$ are 0, ± 1 give the solutions:

$$(x = 0,\ y = 0),\ (x = 1.\ y = 0),\ (x = -1,\ y = 2),\ (x = -1,\ y = -2) \qquad (10)$$

We find now the integral solutions of (9), where neither x nor

$x^3 - 1$ are $0, \pm 1$.

We can easily see that only the following four cases are left:

Case 1

x is odd, and $x = u^2$ $(u \in \mathbb{Z},\ u > 1)$

In this case we must have $x^3 - 1 = 2v^2$ $(v \in \mathbb{Z},\ v > 0)$

Case 2

x is odd, and $x = -u^2$ $(u \in \mathbb{Z},\ u > 1)$

In this case $x^3 - 1 = -2v^2$ $(v \in \mathbb{Z},\ v > 0)$

Case 3

$x = 2u^2$ $(u \in \mathbb{Z},\ u > 0)$

In this case $x^3 - 1 = v^2$ $(v \in \mathbb{Z},\ v > 1)$

Case 4

$x = -2u^2$ $(u \in \mathbb{Z},\ u > 0)$

In this case $x^3 - 1 = -v^2$ $(v \in \mathbb{Z},\ v > 1)$

We treat each case separately as follows:

Case 1: $x^3 - 1 = 2v^2$, where $v \in \mathbb{Z}$, $v > 0$.

We have: $x^3 = (1 + v\sqrt{-2})(1 - v\sqrt{-2})$

The number field $\mathbb{Q}(\sqrt{-2})$ has unique factorization and its units are ± 1, which are all cubes in $\mathbb{Q}(\sqrt{-2})$. Furthermore $1 + v\sqrt{-2}$, $1 - v\sqrt{-2}$ are coprime integers in $\mathbb{Q}(\sqrt{-2})$, since if p is a prime integer in $\mathbb{Q}(\sqrt{-2})$ dividing both factors, then p divides their sum, that is, $p = \pm\sqrt{-2}$. But $\pm\sqrt{-2}$ does not divide either factor.

Therefore there are rational integers κ, λ such that:

$$1 + v\sqrt{-2} = (\kappa + \lambda\sqrt{-2})^3$$

So $\kappa(\kappa^2 - 6\lambda^2) = 1$ and $\lambda(3\kappa^2 - 2\lambda^2) = v$

hence: $\kappa = 1$, $\lambda = 0$, $v = 0$

Therefore the equation $x^3 - 1 = 2v^2$ has no integral solution for $v > 0$.

Case 2: $x^3 - 1 = -2v^2$, where $v \in \mathbb{Z}$, $v > 0$

L. Aubry and E. Fauquembergue have proved that the only solutions of $x^3 - 1 = 2v^2$ are:

$$(x = -1,\ v = \pm 1),\ (x = 1.\ v = 0),\ (x = -23,\ v = \pm 78)$$

(See [16], Vol. 2, p.p. 538)

The only acceptable solutions in this case are

$$(x = -1,\ v = 1)$$

We eliminate all the others, since v must be strictly positive and x strictly negative.

For $(x = -1,\ v = 1)$, we find the solutions

$$(\alpha = 1, \beta = 0),\quad (\alpha = 1,\ \beta = 4)$$

Case 3: $x^3 - 1 = v^2$, where $v \in \mathbb{Z}$, $v > 1$

We have: $x^3 = (1 + iv)(1 - iv)$

The number field $\mathbb{Q}(\sqrt{-1})$ has unique factorization and its units are $\{\pm 1, \pm i\}$ which are allcubes in $\mathbb{Q}(\sqrt{-1})$.

Furthermore, $1 + iv$, $1 - iv$ are coprime integers in $\mathbb{Q}(\sqrt{-1})$.

For, let $a + bi$ be a common factor of $1 + iv$, $1 - iv$.

Then $a + bi$ divides their sum, that is, $a + bi$ divides 2.

Taking norms we find $a^2 + b^2 = 4$

So the candidates common factors are:

$$\pm 1, \pm i, \pm 2i, \pm 2, \pm 1 \pm i$$

It is clear that $\pm 2i$, ± 2 are not common factors.

Also the case where $\pm 1 \pm i$ is a common factor leads to that, where v is odd, and so x is even.

In this case, it is easily seen that $x^3 - 1 = v^2$ has no integral solution.

Therefore, we may consider that the only common factors are the units of $\mathbb{Q}(\sqrt{-1})$. Hence $1 + iv$, $1 - iv$ are coprime integers, and so there are rational integers A, B such that

$$1 + iv = (A + iB)^3$$

Thus $A(A^2 - 3B^2) = 1$

and so $A = 1,\ B = 0,\ v = 0$

Therefore, $x^3 - 1 = v^2$ has no integral solution for $v > 1$.

Case 4: $x^3 - 1 = -v^2$, where $v \in \mathbb{Z}$, $v > 1$

This is a classical equation solved by Euler ([16], Vol 2, p.p. 533-534). The only solutions are:

$$(x = 0, v = \pm 1), (x = -2, v = \pm 3), (x = 1, v = 0)$$

The only acceptable solution in this case is

$$(x = -2, v = 3)$$

which gives the solutions

$$(\alpha = 2, \beta = 2), \quad (\alpha = 2, \beta = 14)$$

Now since the trivial solutions (10) give:

$$(\alpha = 0, \beta = 0), (\alpha = -1, \beta = 2), (\alpha = 1, \beta = 4), (\alpha = 1, \beta = 0)$$

the only solutions of (7) are:

$$\begin{aligned} &(\alpha = 0, \beta = 0), (\alpha = -1, \beta = 2), (\alpha = 1, \beta = 4) \\ &(\alpha = 1, \beta = 0), (\alpha = 2, \beta = 2), (\alpha = 2, \beta = 14) \end{aligned} \tag{11}$$

2.6. Now we find $\gamma_2(\omega + 1)$ in terms of coefficients κ, λ of the equation (4).

Note, that:

$$-\gamma_2(\omega+1) = \sum_{i \neq j} \rho_i^4 \rho_j^4$$

and one easily deduces that

$$-\gamma_2(\omega+1) = \left\{ \left(\sum_{i \neq j} \rho_i \rho_j \right)^2 - 2\rho_1\rho_2\rho_3 \sum \rho_i \right\}^2 - 2\rho_1^2\rho_2^2\rho_3^2 \left\{ \left(\sum \rho_i \right)^2 - 2 \sum_{i \neq j} \rho_i \rho_j \right\}$$

and so, by the equation (4),

$$-\gamma_2(\omega+1) = \lambda^4 - 8\lambda^2\kappa + 8\kappa^2 + 16\lambda$$

Putting $\kappa = -2\alpha$, $\lambda = 2\beta$ to the above formula, we find

$$-\gamma_2(\omega+1) = 2^4 (\beta^4 + 4\alpha\beta^2 + 2\alpha^2 + 2\beta)$$

For the integral solutions (α, β) of the equation (7), given by (11), one finds that:

$$-\gamma_2(\omega + 1) = 0, \ 2^5 .3, \ 2^5 .3.5.11, \ 2^5, \ 2^6 .3.5, \ 2^6 . 3.5.23.29,$$

respectively.

By the (Lem III. 2.1), $-\gamma_2(\omega + 1) > 0$. Therefore there are only

five remaining cases to be considered, and these are given by the following table:

α	-1	1	1	2	2
β	2	4	0	2	14
$-\gamma_2(\omega+1)$	$2^5.3$	$2^5.3.5.11$	2^5	$2^6.3.5$	$2^6.3.5.23.29$

On the other hand we have already proved, (see I. 5.2.11) that:

$$q^{-1/6} - 256q^{1/3} < -\gamma_2(\omega+1) \qquad (12)$$

where $q = e^{-2n\sqrt{p}}$.

Weber also proved that:

$$-\gamma_2(\omega+1) < q^{-1/6} - 256q^{1/3} + \frac{8q^{1/3}}{1-8q^{1/2}-q} + \frac{2^{12}q^{5/6}}{1-q} \qquad (13)$$

(see, [48] , § 125, p.p. 461-2) ,

and having used the inequalities (12), and (13), he deduced that:

$$\begin{aligned}
-\gamma_2\left(\frac{3+\sqrt{-19}}{2}\right) &= 2^5.3 \\
-\gamma_2\left(\frac{3+\sqrt{-67}}{2}\right) &= 2^5.3.5.11 \\
-\gamma_2\left(\frac{3+\sqrt{-11}}{2}\right) &= 2^5 \\
-\gamma_2\left(\frac{3+\sqrt{-43}}{2}\right) &= 2^6.3.5 \\
-\gamma_2\left(\frac{3+\sqrt{-163}}{2}\right) &= 2^6.3.5.23.29
\end{aligned} \qquad (14)$$

Note, that the values on the right hand sides of (14) coinside

with the values of the last row of the above table. Therefore, by the bijectivity of the j-function, we deduce that, if $h(-p) = 1$, $p \equiv 3 \pmod 8$, $p > 3$, then we must have:

$$p = 11,\ 19,\ 43,\ 67,\ 163\ .$$

Conversely, if p takes the above values, $j(\omega)$ is a negative rational integer, and since $K_2 = k_1(j(\omega))$ we have $[K_2 : K_1] = 1$, that is $h(-p) = 1$.

This completes the proof of the (Th. III. 1.1) .

CHAPTER IV

ELLIPTIC CURVES WITH INFINITELY MANY RATIONAL POINTS

1. The Weak Mordell-Weil Theorem, and the group of 2-coverings U of an elliptic curve.

1.1 The Weak Mordell-Weil Theorem

Let E be an elliptic curve defined over $\mathbb{Q}$ with Weierstrass form: $y^2 = h(x) = x^3 - Ax - B$,

where $A, B \in \mathbb{Z}$.

By the Mordell-Weil theorem, $E(\mathbb{Q})$ is finitely generated and its subgroup $E(\mathbb{Q})^f$ of rational points of finite order is finite.

We denote by r the number of independent generators of $E(\mathbb{Q})$ of infinite order, and by r_2 the number of independent generators of finite even order. Clearly $r_2 = 0$, 1 or 2 if the polynomial h (x) has o, 1, or 3 rational zeros,respectively.

Now we state the following result, which was proved by Weil, in the general case where E is defined over a number field K. (See Lang [29] , p.p. 101, V, § 1).

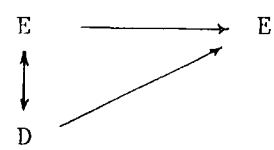
The Weak Mordell-Weil Theorem (Th. IV. 1.1.1)

The quotient group $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.
In fact, it has order 2^{r+r_2}.

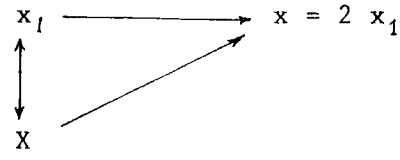
1.2 The group of 2-coverings U of an elliptic curve

Let E be an elliptic curve defined over $\mathbb{Q}$. Following Cassel's definition (see Cassels [9]) we say that there is a 2-covering U of E if there is a curve D defined over $\mathbb{Q}$ and a commutative triangle:

U :



with associated generic points



where the map $X \dashrightarrow x$ is over the rationals, and $X \leftrightarrow x_1$ is over the complex numbers. We shall say that another curve D' with generic point X' gives the same 2-covering on E, if and only if, there is a birational mapping

$$X \longleftrightarrow X'$$

over the rationals and a point P on E with $2P = \mathcal{O}$, such that the diagram

$$\begin{array}{ccc} x_1 & \longleftrightarrow & x_1' = x_1 + P \\ \updownarrow & & \updownarrow \\ X & \longleftrightarrow & X' \end{array}$$

is commutative.

There is also a natural structure of an abelian group on the 2-coverings U of E, inherited from the law of composition of the curves D regarded as homogeneous spaces (see Weil [49]). We denote by G the group of 2-coverings U of E. Every element of G other than the identity has order 2.

We are interested here in a special subgroup of G, which we denoted by G^{ra} , consisted of 2-coverings U of E for which D has a rational point (C.F. Birch and Swinnerton-Dyer, in [6], denote this group by G' and is clearly a subgroup of those 2-coverings U for which D has a point in each p-adic field).

Weil has also proved that:

Theorem (Th. IV. 1.2.1)

The group G^{ra} is isomorphic to $E(\mathbb{Q})/2E(\mathbb{Q})$, and consequently $|G^{ra}| = 2^{r+r_2}$.

Birch and Swinnerton-Dyer have found an effective method under which one can specify 2-coverings U of an elliptic curve E (See Birch and Swinnerton-Dyer [6]).

In the next we quote some of their results.

Lemma (Lem. IV. 1.2.2) (See [6] I , Lemmas 1, 2 p.p. 9 - 11)

(i) If D is a curve corresponding to a 2-covering U in G^{ra} ,

then we can take D in the form

$$y^2 = g(x) = ax^4 + bx^3 + cx^2 + dx + e \qquad (1)$$

where a, b, c, d, e are rational.

Furthermore, the curve (1) is a 2-covering of

$$y^2 = x^3 - 27Ix - 27J \qquad (2)$$

where $I = 12ae - 3bd + c^2$, $J = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3$ which are called the invariants of (1).

And conversely, any 2-covering of (2) has invariants $I\lambda^4$, $J\lambda^6$ for some rational λ .

(ii) Two curves D and D^* of the form (1) give the same covering, if and only if, there are rational numbers $\alpha, \beta, \gamma, \delta, \mu$ such that:

$$g(x) = \mu^2(\gamma x + \delta)^4 g^*\left(\frac{\alpha x + \beta}{\gamma x + \delta}\right)$$

Clearly, if D, D^* are equivalent, then g(x), $g^*(x)$ have the same splitting field.

(iii) If g(x) has a rational zero, it gives rise to the trivial 2-covering defined by the map $X \longrightarrow 2X$ of E onto itself.

2. A specific example of an infinite series of elliptic curves with infinitely many rational points.

We set $\omega = \frac{1 + \sqrt{-p}}{2}$, where p is a rational prime such that $p \equiv 3 \pmod 4$, and $p > 3$. Let $K = \mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-p})$.

We recall some general facts from the Chapters I and II.

These are:

(i) $j(\omega)$ is a real algebraic integer less than zero (Th. I. 5.2.12) .

(ii) The Hilbert class-field $K_1 = K(j(\omega))$ (Th. II. 2.2)

(iii) $h(-p) = [K_1 : K] = \text{odd}$ (Th. II. 4.2)

(iv) $[K_2 : K_1] = \begin{cases} 3, & \text{if } p \equiv 3 \pmod 8 \\ 1, & \text{if } p \equiv 7 \pmod 8 \end{cases}$, and $K_2' = K_2$ (Th. II. 4.5)

Now we also recall some results from the Chapter III which depend only on the fact h(-p) = odd and not on the special case where h(-p) = 1.

These are:

(v) $-f_2^{24}(\omega)$ is the unique real root of the equation

$$(t - 16)^3 = j(\omega)\, t \qquad (1)$$

which is also positive. Furthermore $f_2^{24}(\omega) \in K_2$.

In particular if $p \equiv 3 \pmod 8$ then $K_2 = K_1(f_2^{24}(\omega))$ (Th. III. 2.2)

(vi) $-if_2^{12}(\omega)$, $e^{3\pi i/4} f_2^6(\omega)$ are real and positive and also lie in K_2. (From a part of the proof of (Th. III. 2.3.1)).

Lemma (Lem. IV. 2.1)

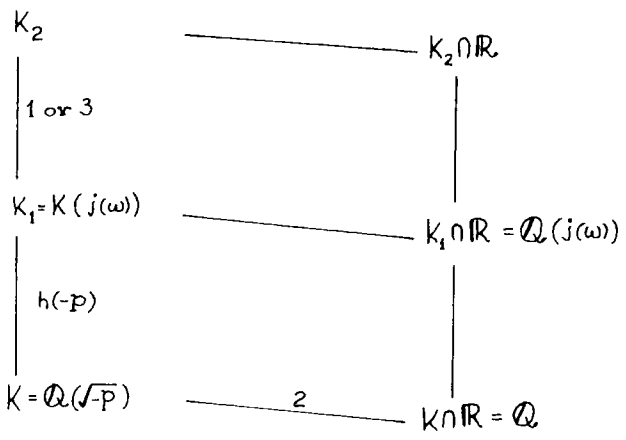
$K_2 \cap \mathbb{R}$ is an odd extension of $\mathbb{Q}$; in fact

$$[K_2 \cap \mathbb{R} : \mathbb{Q}] = \begin{cases} h(-p), & \text{if } p \equiv 7 \pmod 8 \\ 3h(-p), & \text{if } p \equiv 3 \pmod 8 \end{cases} .$$

Proof

First we prove that $[K_1 \cap \mathbb{R} : \mathbb{Q}] = h(-p)$.

Clearly, $K \cap \mathbb{R} = \mathbb{Q}$, and $K_1 \cap \mathbb{R} = \mathbb{Q}(j(\omega))$.



Note that $[K_1 : K_1 \cap \mathbb{R}] = [\mathbb{Q}(j(\omega), \sqrt{-p}) : \mathbb{Q}(j(\omega))] = 2$

and since $[K_1 : \mathbb{Q}] = 2h(-p)$, we have $[K_1 \cap \mathbb{R} : \mathbb{Q}] = h(-p)$.

Suppose that $p \equiv 7 \pmod 8$, then $K_2 = K_1$ and so

$[K_2 \cap \mathbb{R} : \mathbb{Q}] = h(-p)$.

Now suppose that $p \equiv 3 \pmod 8$, then $[K_2 : K_1] = 3$, and

$K_2 = K_1(f_2^{24}(\omega)) = \mathbb{Q}(\sqrt{-p}, j(\omega), f_2^{24}(\omega))$

Clearly $K_2 \cap \mathbb{R} = \mathbb{Q}(j(\omega), f_2^{24}(\omega))$

and so $[K_2 : K_2 \cap \mathbb{R}] = 2$

Since $[K_2 : K_1 \cap \mathbb{R}] = [K_2 : K_1][K_1 : K_1 \cap \mathbb{R}] = 3.2$, and

$[K_2 : K_2 \cap \mathbb{R}] = 2$, we have $[K_2 \cap \mathbb{R} : K_1 \cap \mathbb{R}] = 3$

Therefore, $[K_2 \cap \mathbb{R} : \mathbb{Q}] = [K_2 \cap \mathbb{R} : K_1 \cap \mathbb{R}][K_1 \cap \mathbb{R} : \mathbb{Q}] = 3h(-p)$

So the lemma holds.

Now we prove that:

Lemma (Lem IV. 2.2)

$\gamma_3(\omega) \in K_1$. In particular,

$\gamma_3(\omega) = \lambda\sqrt{-p}$, for some $\lambda \in K_1 \cap \mathbb{R}$.

Proof

From (Th. I. 4.5.6), and $\gamma_3^2(\tau) = j(\tau) - 1728$ we deduce that $\gamma_3(\tau)$ has at each cusp of $\hat{\Gamma}(2)$ Fourier expansion with coefficients in $\mathbb{Q}$, and therefore by Söhngen's theorem $\gamma_3(\omega) \in K_2$

Now note that $\gamma_3(\omega)$ is a zero of the polynomial

$$\phi(x) = x^2 - j(\omega) + 1728 \in K_1[x] .$$

Since $j(\omega) < 0$, $\gamma_3(\omega)$ is a pure imaginary number.

Also from the tower of fields

$$K_2 \supset K_1(\gamma_3(\omega)) \supset K_1$$

since $[K_2 : K_1] = 1$ or 3 , we have $\phi(x)$ is reducible over K_1 and so $\gamma_3(\omega) \in K_1$

Now since $K_1 = \mathbb{Q}(\sqrt{-p})(j(\omega))$, and $j(\omega)$ is real, we have

$\gamma_3(\omega) = \lambda\sqrt{-p}$ for some $\lambda \in K_1 \cap \mathbb{R}$.

Theorem (Th. IV. 2.3)

The curve D: $-py^2 = x^4 - 64$ has a $\mathbb{Q}$-rational point.

Proof

First, we prove that D is soluble in $K_2 \cap \mathbb{R}$.

It is easily seen that the equation $(t - 16)^3 = j(\omega)\, t$

can be written as:

$$j(\omega) - 1728 = \frac{(t - 64)(t + 8)^2}{t} ,$$

that is, $\gamma_3^2(\omega) \frac{t}{(t+8)^2} = t - 64$.

Note that in view of (V) and, (VI) we have

$$\left\{ \gamma_3(\omega) \frac{-i f_2^{12}(\omega)}{-f_2^{24}(\omega)+8} \right\}^2 = \left\{ e^{3\pi i/4} f_2^6(\omega) \right\}^4 - 64$$

and from (Lem. IV. 1.1), we deduce that

$$\left\{ \sqrt{-p} \cdot \lambda \frac{-i f_2^{12}(\omega)}{-f_2^{24}(\omega)+8} \right\}^2 = \left\{ e^{3\pi i/4} f_2^6(\omega) \right\}^4 - 64$$

which means that D has a $K_2 \cap \mathbb{R}$ -rational point, namely

$$(x, y) = \left(e^{3\pi i/4} f_2^6(\omega) , \lambda \cdot \frac{-i f_2^{12}(\omega)}{-f_2^{24}(\omega)+8} \right)$$

We now prove that D has a $\mathbb{Q}$ -rational point. We need first to recall the following facts concerning divisors of an elliptic curve D defined over the rationals. (See Farkas and Kra [17] , p.p.67, 90, III. 4)

There is a fundamental isomorphism $D(\mathbb{C}) \xrightarrow{\sim} \tilde{D}_o = D_o / D_{pr}$ given by: $P \longmapsto [P] - [\mathcal{O}]$,

where D_o is the group of divisors of D of degree 0, and D_{pr} is the group of principal divisors, that is the group of divisors of degree 0, which are divisors of functions defined on D.

This induces a bijection

$$h : D(\mathbb{C}) \longleftrightarrow \tilde{D}_1 ,$$

where $\tilde{D}_1$ is the set of divisor classes of degree 1. Clearly h preserves the action by the Galois group of $\mathbb{C}$ and from this we deduce a bijection:

$$D(\mathbb{C})^{Gal(\mathbb{C}/\mathbb{Q})} \longleftrightarrow \tilde{D}_1^{Gal(\mathbb{C}/\mathbb{Q})}$$

between the $\mathbb{Q}$ -rational points of E and the rational divisors of degree 1.

We return now to the problem in hand. Let P be the $K_2 \cap \mathbb{R}$ -rational point of D. Since $K_2 \cap \mathbb{Q}$ is of odd degree over $\mathbb{Q}$, the sum, Σ , of conjucates of P over $\mathbb{Q}$ provides a rational divisor of odd degree .

We denote by $Q = (2\sqrt{2}, 0)$, $Q' = (-2\sqrt{2}, 0)$.

Clearly $Q + Q'$ is a rational divisor of degree 2 and

therefore

$$\mathfrak{Z}_1 = \mathfrak{Z} - \frac{\deg \mathfrak{Z} - 1}{2}.(Q + Q')$$

is a rational divisor of degree 1. Hence, by the above bijection, D has a $\mathbb{Q}$-rational point, as required.

The Final Result (IV. 2.4)

The curve $E : y^2 = x^3 + p^2 x$ has infinitely many rational points.

Proof

In view of the previous discussion, and since $\gamma_2 = 1$ it suffices to prove that $|G^{ra}| \geq 3$, that is enough to find two non-trivial, inequivalent, 2-coverings U of E.

We show that the curves

$$D : -py^2 = x^4 - 64,$$

and

$$\tilde{D} : y^2 = -x^4 + 4p^2$$

are as required.

The curve $\tilde{D}$ has the obvious rational points

$$(x = 0, y = \pm 2p) \quad .$$

The following diagram shows how the curve D is rationally transformed to the curve $D' : y^2 = -\frac{1}{p} x^4 + \frac{1}{2^2 . 3^4} p^3$.

$$D \xrightarrow{(x, y) \longmapsto \left(\frac{12}{p} x, \left(\frac{12}{p}\right)^2 y\right)} D'$$

Also the following diagram shows how the curve $\tilde{D}$ is rationally transformed to the curve $\tilde{D}' : y^2 = -4p^2 x^4 + \frac{1}{2^4 . 3^4}$

$$\tilde{D} \xrightarrow{(x, y) \longmapsto (2^2 . 3 p x, 2^3 . 3^2 p y)} \tilde{D}'$$

In view of (Lem. IV. 1.2.2) the invariants of the quartics D', and $\tilde{D}'$ are:

$$I = -\frac{p^2}{27} \quad , \quad J = 0$$

So, D and $\tilde{D}$ are both 2-coverings of the curve

$$y^2 = x^3 - 27Ix \quad ,$$

that is, $y^2 = x^3 + p^2 x$

Clearly, they are not trivial, since $-\frac{1}{p}x^4 + \frac{64}{p}$ and $-x^4 + 4p^2$ have no rational roots.

Also they are inequivalent, since the splitting fields of the above polynomials over $\mathbb{Q}$ differ.

This proves our claim.

———— • ————

REFERENCES

1. T.M. Apostol, "Modular Functions and Dirichlet Series in Number Theory", Springer-Verlag, New York Heidelberg, Berlin, (1976)

2. W.L. Baily, Jr., "Introductory lectures on Automorphic forms", Iwanami Shoten, Publishers and Princeton University Press, (1973)

3. A. Baker, "Linear forms in the logaritms of algebraic numbers", Mathematika, 13 (1966), p.p. 204-216.

4. B.J. Birch, "Weber's class invariants", Mathematika, 16 (1969), 283-94.

5. B.J. Birch, "Diophantine Analysis and Modular Functions", Proceedings of the Conference of Algebraic Geometry. (Bombay, 1968), 35-42.

6. B.J. Birch and H.P.F. Swinnerton-Dyer, "Notes on elliptic curves" I., J. für reine u. angew, Math. 212 (1962), 7-25. II., J. für reine u. angew, Math. 218 (1965), 79-108.

7. B.J. Birch, "Conjectures Concerning Elliptic Curves", Proc. of Symposia in Pure Math., V. VIII, Theory of Numbers, (1965), p.p. 106-112.

8. L. Carlitz, "Note on the class number of quadratic fields". Duke Math. J. 22 (1955), 589-593.

9. J.W.S. Cassels, "Arithmetic on curves of genus 1", II. A general result. J. reine, u. angew. Math. 203 (1960), 174-208.

10. J.W.S. Cassels, "Diophantine Equations with special reference to Elliptic Curves". Survey Article. J. London Math. Soc. 41, (1966), 193-291.

11. K. Chandrasekharan, "Arithmetical Functions", Springer-Verlag, (1970)

12. J. Coates and A. Wiles, "On the Conjecture of Birch and Swinnerton-Dyer". Inventiones math. 39, 223-251 (1977).

13. J. Coates and C. Goldstein, "Some remarks on the main conjecture for elliptic curves with complex multiplication". Am. J. of Math., V 105, Number 2, April (1983).

14. M. Deuring, "Die Klassenkörper der komplexen Multiplication", Enz. Math. Wiss. Band I_2,Heft 10, Teil II, 23 (Stuttgart, 1958).

15. M. Deuring, "Imaginäre quadratische Zahlkörper mit der Klassenzahl Eins", Invent. Math. 5 (1968), 169-179.

16. L.E. Dickson, "History of the theory of numbers", 3 volumes, Stechert, New York, (1934).

17. H.M. Farkas, I. Kra, "Riemann Surfaces", Springer-Verlag, B.H. New York, 71, (1980).

18. S. Gelbart, "Elliptic Curves and Automorphic Representations" Advances in Math. 21, 235-292, (1976).

19. D.M. Goldfeld, "The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer".

20. E. Grosswald, "L-functions and quadratic fields with unique factorization".

21. R.C. Gunning, "Lectures on Modular Forms", Annals of Mathematics Studies, Number 48, Princeton, New Jersey, P.U. Press, (1962).

22. H. Hasse, "Number Theory", Springer-Verlag, Berlin Heid., New York, 1980.

23. K. Heegner, "Diophantische Analysis und Modulfunktioner" Math. Z. 56, (1952), 227-253.

24. H. Heilbronn - E.H. Linfoot, "On the imaginary quadratic corpora of class-bumber one", Quart. J. Math. Oxford Ser. 5 (1934), 293-301.

25. K. Ireland - M. Rosen, "A Classical Introduction to Modern Number Theory", Springer-Verlag, (1982).

26. G.J. Janusz, "Algebraic number fields", Ac. Press, New York and London, (1973).

27. S. Lang, "Introduction to Algebraic Geometry", Interscience Pub., INC., New York, (1958).

28. S. Lang, "Elliptic Functions", Addition-Wesley Pub. Co., Inc., (1973)

29. S. Lang, "Elliptic Curves Diophantine Analysis", Springer-Verlag, B.H. New York (1978)

30. S. Lang, "Algebraic Number Theory", Addison-Wesley Pub. Co., INC, (1970).

31. D.A. Marcus, "Number Fields", Springer-Verlag, (1977)

32. A.W. Mason, "Lattice subgroups of free congruence groups", Glasgow, M.J., V.10, (1969), 106-115.

33. A. Ogg, "Modular forms and Dirichlet series", W.A. Benjamin, INC, (1969).

34. H. Rademacher, "Topics in Analytic Number Theory", Springer-Verlag, B.H. New York, (1973).

35. R. Rankin, "Modular forms and functions", Cambridge U. Press, (1977).

36. A. Robert, "Elliptic Curves", Lecture Notes in Math, Springer-Verlag, 326, (1973)

37. B. Schoeneberg, "Elliptic Modular Functions", Springer-Verlag, B.H. New York (1974)

38. J.P. Serre, "A course in Arithmetic", Springer-Verlag, New York, Heidelberg, Berlin, (1973).

39. I.R. Shafarevich, "Basic Algebraic Geometry", Springer-Verlag, B.H. New York, (1974).

40. G. Shimura, "Introduction to the Arithmetic theory of Automorphic functions", Iwanami Shoten, Pub. and Princeton U. Press, (1971).

41. C. Siegel, "A simple proof of $\eta(-\frac{1}{\tau}) = \eta(\tau)\sqrt{\tau/i}$ " Mathematika 1, (1954).

42. C. Siegel, "Abschätzung von Einheiten" Nachr. Akad. Wiss. Göttingen (1969) p.p. 71-86 .

43. C. Siegel, "Zum Beweise des Starkschen Satzes", Invent. Math., 5 (1968) ,180-191.

44. H. Söhngen, "Zur Komplexen Multiplication" Math. Annallen 111, (1935), 302-328.

45. H.M. Stark, "A complete determination of the complex quadratic fields of class-number one", Michigan Math. J. 14 (1967), 1-27.

46. H.P.F. Swinnerton-Dyer "Analytic Theory of Abelian Varieties" London Math. Soc. Lecture Notes. 14, Cambridge U. Press, (1974)

47. J.T. Tate, "The Arithmetic of Elliptic Curves", Inventiones Math. 23, (1974), 179-206.

48. H. Weber, "Lehrbuch der Algebra", Vol. I., II, III, Third ed., Chelsea Pub. Co., New York, N.Y. (1961)

49. A. Weil, "On algebraic groups and homogeneous spaces" Amer. J. Math. 77 (1955), 493-512.

50. K. Wohlfahrt, "An extension of F. Klein's level concept", Illinois J. of Math. 8, (1964), 529-535.

———— ∘ ————