HILBERT MODULAR FORMS OF WEIGHT 1/2

Thesis by

Sever Achimescu

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

2005

(Defended September 27, 2004)

Acknowledgement

I am grateful to my advisor, Professor Dinakar Ramakrishnan, for his guidance and encouragement.

I thank Caltech for its financial support.

Abstract

Let

$$H = \sum_{\mathcal{N},\chi} \mathcal{M}_{\frac{1}{2}}(\mathcal{N}, \chi)$$

be the space of Hilbert modular forms of half integral weight of all levels $\mathcal{N}$ and characters χ.

We denote by $\varphi_{\mathcal{N}} : \mathcal{O}_F \to \mathbf{C}$ a periodic function of period $\mathcal{N}$.

Let Θ be the $\mathbf{C}$-linear space of the functions $f : \mathcal{H} \times \mathcal{H} \to \mathbf{C}$,

$$f(z) = \sum_{t} \sum_{\xi \in \mathcal{O}_F} \varphi_{\mathcal{N}_t}(\xi) exp(t\pi i(\xi^2 z_1 + \xi^{'2} z_2))$$

where, for each f, $t \in \mathcal{O}_F$ runs through a finite subset of totally positive integers of F.

Main Theorem.

$$H = \Theta$$

Using this theorem, for some fixed F's, an explicit basis can be found. Some examples are given in Chapter4.

Contents

Chapter 1

Introduction

Classically, a modular form of weight $k \in \mathbf{Z}$ for a congruent subgroup $\Gamma := \Gamma_0(N) := \{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, N|c\} < SL_2(\mathbf{Z})$ is a holomorphic function f on the upper-half plane $\mathbf{H} := \{z \in \mathbf{C}, \mathrm{Im}z > 0\}$ satisfying

$$f(\gamma z) = (cz + d)^k f(z), \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$$

and an additional property called "holomorphicity at the cusps." Using the natural inner product, namely, the Petterson inner product on the $\mathbf{C}$-vector space of modular forms, we get finite a dimensional Hilbert space for each pair (Γ, k). There are Hecke operators $\{T(p)\}_{p \not| N \text{ prime}}$ which preserve these spaces.

A generalization is when we allow $k \in \mathbf{Z}[\frac{1}{2}]$ and we get the half integral weight modular forms. Shimura introduced a family of corresponding Hecke operators $\{T(p^2)\}_{p \text{ prime}}$. In [Serre-Stark], Serre and Stark proved a theorem which gives explicit basis consisting of theta functions for some spaces of half integral weight modular forms.

The Hilbert modular forms (of half integral weight) are modular forms (of half integral weight) of several variables. The main result in my dissertation is an analog, for certain real quadratic fields of class number one, of the theorem of Serre-Stark which gives algorithms to compute basis of spaces of half integral weight modular forms over $\mathbf{Q}$. An alternative proof of a part of the Serre-Stark theorem, which was outlined (using adellic representations) by Pierre Deligne in a letter to Jean Pierre Serre, is expanded and generalized in this thesis to some quadratic fields of class number one in Chapter 3. Some of the results of Serre and Stark over $\mathbf{Q}$, which Deligne implicitly assumed, require different arguments over F. In particular, one need to use certain nontrivial, structural results of Goro Shimura on Hilbert modular forms of half integral weight.

There is already a vast generalization of the Serre-Stark theorem in a slightly different form, due to Shimura, valid over all totally real fields, but this method seems to only give generators, not a basis. The result in Chapter 3 is in a more explicit form and hopefully more suitable for applications. See Chapter 4 for examples.

In Chapter 5 we define the congruent number problem over F and we take a few steps towards generalizing Tunnell's results over $\mathbf{Q}$. Here the generalization is not trivial, since already for $\mathbf{Q}(\sqrt{\mathbf{2}})$ there are examples of $\mathbf{Q}(\sqrt{\mathbf{2}})$-congruent numbers α such that the associated elliptic curve E_α : $y^2 = x^3 - \alpha^2 x$ over $\mathbf{Q}(\sqrt{\mathbf{2}})$ has zero rank; α corresponds to torsion points which E_α acquires over $\mathbf{Q}(\sqrt{\mathbf{2}})$.

Chapter 2

Preliminaries

Let F be a totally real number field with class number one and discriminant D; $F = \mathbf{Q}(\sqrt{d_0}) = \mathbf{Q}(\sqrt{D})$ with d_0 square free and such that $\mathcal{O}_F = \mathbf{Z}[\sqrt{d_0}]$, where $\mathcal{O}_F$ denotes the ring of integers of F. The two real embeddings are $a + b\sqrt{d_0} \mapsto a \pm b\sqrt{d_0}$. The discriminant (of F) is $D_{F/\mathbf{Q}} = d_0$, the different is $\mathcal{D} := \mathcal{D}_{F/\mathbf{Q}} = 2\sqrt{d_0}\mathcal{O}_F$ and the inverse different is $\mathcal{D}^{-1} = \frac{1}{2\sqrt{d_0}}\mathcal{O}_F$.

For P prime ideal of $\mathcal{O}_F$ we denote $P = \varpi\mathcal{O}_F$, $\varpi \in \mathcal{O}_F$.

Put $SL_2(\mathcal{O}_F) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in \mathcal{O}_F, ad - bc = 1\}$. For $\xi = m + n\sqrt{d_0} \in \mathcal{O}_F$ we denote $\xi' = m - n\sqrt{d_0}$ its conjugate.

For $\mathcal{N}$ an ideal in $\mathcal{O}_F$ we denote

$$\Gamma_0(\mathcal{N}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathcal{O}_F), c \in \mathcal{N}\}.$$

Put $\mathcal{H} = \{z \in \mathbf{C}, \mathrm{Im}z > 0\}$ and $z = (z_1, z_2) \in \mathcal{H} \times \mathcal{H}$.

$\Gamma_0(\mathcal{N})$ acts on $\mathcal{H} \times \mathcal{H}$ as follows: first we view $\Gamma_0(\mathcal{N}) \hookrightarrow GL_2(\mathbf{R}) \times$

$GL_2(\mathbf{R})$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix})$$

then $GL_2(\mathbf{R}) \times GL_2(\mathbf{R})$ acts on $\mathcal{H} \times \mathcal{H}$ componentwise:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}, (z_1, z_2) \mapsto (\frac{az_1 + b}{cz_1 + d}, \frac{a'z_2 + b'}{c'z_2 + d'})$$

All square roots of numbers in $\mathbf{C} - \{x < 0\}$ are to be taken in the right half-plane.

Define $\theta : \mathcal{H} \times \mathcal{H} \to \mathbf{C}$ as follows:

$$\theta(z) := \sum_{\xi \in \mathcal{O}_F} exp(\pi i(\xi^2 z_1 + \xi'^2 z_2))$$

Observe that θ is holomorphic on $\mathcal{H} \times \mathcal{H}$.

Recall that a function f on an open set in $\mathbf{C}^n$ is said to be holomorphic iff it has an absolutely convergent power series expansion in each compact polydisc in that open set. We have

$$|\theta(z)| = |\sum_{\xi \in \mathcal{O}_F} exp(\pi i \xi^2 z_1) exp(\pi i \xi'^2 z_2)| \leq$$

$$|\sum_{\xi \in \mathcal{O}_F} exp(2\pi i \xi^2 z_1)|^{\frac{1}{2}} |\sum_{\xi \in \mathcal{O}_F} exp(2\pi i \xi'^2 z_2)|^{\frac{1}{2}}$$

Because the one-dimensional theta function

$$\mathcal{H} \to \mathbf{C}\,,\ z \mapsto \sum_{n\in\mathbf{Z}} exp(2\pi i n^2 z)$$

is holomorphic, the series in the righthand side of the above inequality converge absolutely on each compact (on $\mathcal{H}$), therefore the series defining θ converges absolutely on each compact (in $\mathcal{H}\times\mathcal{H}$).

For a prime ideal $p\mathcal{O}_F$ and $\beta \in \mathcal{O}_F$ we define a *quadratic symbol*

$$(\frac{\beta}{p\mathcal{O}_F}) = +1 \ \text{ if}\beta \text{ is a square in } (\mathcal{O}_F/p\mathcal{O}_F)^*$$

$$(\frac{\beta}{p\mathcal{O}_F}) = -1 \ \text{ if}\beta \text{ is a non square in } (\mathcal{O}_F/p\mathcal{O}_F)^*$$

$$(\frac{\beta}{p\mathcal{O}_F}) = 0 \ \text{ if } \beta \in p\mathcal{O}_F$$

We extend it by multiplicativity to all nonzero ideals of $\mathcal{O}_F$. For $0 \neq \alpha \in \mathcal{O}_F$, write $(\frac{\beta}{\alpha}) = (\frac{\beta}{\alpha\mathcal{O}_F})$.

For $\gamma \in \Gamma_0(\mathcal{N})$ we consider the automorphy factor of weight $\frac{1}{2}$, denoted $h(\gamma, z)$, introduced in [Shi2], Proposition 1.2 pg. 285. The definition is intrinsic, though not explicit. This automorphy factor is a holomorphic

function on $\mathcal{H} \times \mathcal{H}$ satisfying $h(\gamma, z)^2 = t(cz_1 + d)(c'z_2 + d')$ where t is a root of unity.

A multiplicative *character* modulo $\mathcal{N}$ is a group homomorphism $\chi : (\mathcal{O}_F/\mathcal{N})^* \to \mathbf{C}^*$. We also view a character χ as a periodic function on $\mathcal{O}_F$ by putting $\chi(\nu) = 0$, $\forall \nu \in \mathcal{N}$.

Definition. *A holomorphic Hilbert modular form of weight* $\frac{1}{2}$*, character* χ *and level* $\mathcal{N}$ *is a function* $f : \mathcal{H} \times \mathcal{H} \to \mathbf{C}$ *which is holomorphic, both on* $\mathcal{H} \times \mathcal{H}$ *and at the cusps, and satisfies*

$$f(\gamma z) = \chi(d)h(\gamma, z)f(z) \ , \ \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\mathcal{N}) \, , \, \forall z \in \mathcal{H} \times \mathcal{H}$$

Note that, since in our case $[F : \mathbf{Q}] > 1$, by the Koecher principle, the condition "holomorphic at the cusps" is superfluous. The definition of Hilbert modular forms of weight $\frac{k}{2}$, with k odd integer, is similar; but with $h(\gamma, z)$ replaced by $h(\gamma, z)^k$.

We denote the $\mathbf{C}$-vector space of holomorphic Hilbert modular forms of weight $\frac{1}{2}$, character χ and level $\mathcal{N}$ by $\mathcal{M}_{\frac{1}{2}}(\mathcal{N}, \chi)$.

Following [Shi1], for $f, g \in \mathcal{M}_{\frac{1}{2}}(\mathcal{N}, \chi)$ we define their inner product

$< f, g >$ by

$$< f, g >=\mid \Gamma\backslash\mathcal{H}\times\mathcal{H} \mid^{-1} \int_{\Gamma\backslash\mathcal{H}\times\mathcal{H}} \overline{f(z)}g(z)(y_1y_2)^{\frac{1}{2}}d_H(z)$$

where y =Imz and $d_H(x+iy) = (y_1y_2)^{-2}dx_1dx_2dy_1dy_2$. This integral converges if one of the forms is a cusp form. But in fact $< f, g >$ makes sense, as noted by Deligne, for all f, g in $\mathcal{M}_{\frac{1}{2}}(\mathcal{N})$.

Given a function $f : \mathcal{H}\times\mathcal{H} \to \mathbf{C}$ we denote $f_t : \mathcal{H}\times\mathcal{H} \to \mathbf{C}$, $f_t(z) = f(tz)$ where t totally positive, $t \in \mathcal{O}_F$. Also, for t totally positive, $t \in \mathcal{O}_F$, we define a "quadratic character" χ_t as follows: for $d \in \mathcal{O}_F$, $d \neq 0$,

$$\chi_t(d) = (\frac{t_0}{d}) \text{ if } t_0 \equiv 1(\text{mod}4)$$

$$\chi_t(d) = (\frac{4t_0}{d}) \text{ otherwise}$$

$$\chi_t(u) = 1\,,\ \forall u \in (\mathcal{O}_F)^*$$

where t_0 denotes the square-free part of $N(t)$.

For a character ψ modulo $\mathcal{N}$, define $\theta_\psi : \mathcal{H}\times\mathcal{H} \to \mathbf{C}$ as follows:

$$\theta_\psi(z) := \sum_{\xi\in\mathcal{O}_F} \psi(\xi)exp(\pi i(\xi^2 z_1 + \xi'^2 z_2))$$

Theorem. $\theta_\psi \in \mathcal{M}_{\frac{1}{2}}(4(cond\,\psi)^2, \psi)$.

Proof.

This is Lemma 4.3 pg. 784 of [Shi1]. In particular, $\theta \in \mathcal{M}_{\frac{1}{2}}(4\mathcal{O}_F)$.

Proposition 1. *Let $t \in \mathcal{O}_F$ be totally positive. Then*

$$f \in \mathcal{M}_{\frac{1}{2}}(\mathcal{N}, \chi\chi_t) \Rightarrow f_t \in \mathcal{M}_{\frac{1}{2}}(t\mathcal{N}, \chi)$$

In particular, since $\chi_t^2 = 1$,

$$f \in \mathcal{M}_{\frac{1}{2}}(\mathcal{N}, \chi) \Rightarrow f_t \in \mathcal{M}_{\frac{1}{2}}(t\mathcal{N}, \chi\chi_t)$$

Proof.

Need to prove

$$f_t(\gamma z) = \chi(d)h(\gamma, z)f_t(z) \ , \ \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(t\mathcal{N}) \, , \, \forall z \in \mathcal{H} \times \mathcal{H}$$

Fix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(t\mathcal{N})$ and put $\gamma_t = \begin{pmatrix} a & bt \\ \frac{c}{t} & d \end{pmatrix} \in \Gamma_0(\mathcal{N})$. By hypothesis, $f \in \mathcal{M}_{\frac{1}{2}}(\Gamma_0(\mathcal{N}), \chi\chi_t)$ thus

$$f(\gamma_t tz) = \chi(d)\chi_t(d)h(\gamma_t, tz)f(tz) \ , \ \forall z \in \mathcal{H} \times \mathcal{H}$$

The conclusion follows by noticing that $\gamma_t tz = t\gamma z$ and using the following

Lemma.

$$\chi_t(d)h(\gamma_t, tz) = h(\gamma, z) \ , \ \forall z \in \mathcal{H} \times \mathcal{H}$$

Proof*:*

The squares of both sides are equal, by [Shi2] pg. 286. It suffices to check the sign. Equivalently, since $h(\gamma, z) = \frac{\theta(\gamma z)}{\theta(z)}$, it suffices to check the Proposition for $f = \theta$. But this is a known fact.

Chapter 3

The main result

Let

$$H = \sum_{\mathcal{N},\chi} \mathcal{M}_{\frac{1}{2}}(\mathcal{N},\chi)$$

be the space of Hilbert modular forms of half integral weight of all levels $\mathcal{N}$ and characters χ.

We denote by $\varphi_{\mathcal{N}} : \mathcal{O}_F \to \mathbf{C}$ a periodic function of period $\mathcal{N}$, i.e. $\varphi(x) = \varphi(x+\alpha)\,, \forall x \in \mathcal{O}_F\,, \forall \alpha \in \mathcal{N}$.

Let Θ be the $\mathbf{C}$-linear space of the functions $f : \mathcal{H} \times \mathcal{H} \to \mathbf{C}$,

$$f(z) = \sum_{t} \sum_{\xi \in \mathcal{O}_F} \varphi_{\mathcal{N}_t}(\xi) exp(t\pi i(\xi^2 z_1 + \xi'^2 z_2))$$

where, for each f, $t \in \mathcal{O}_F$ runs through a finite subset of totally positive integers of F.

Main Theorem.

$$H = \Theta$$

Proof:

The inclusion

$$\Theta \subseteq H$$

follows from **Proposition 1** of the previous chapter and the following

Lemma. *The function*

$$z \mapsto \sum_{\xi \in \mathcal{O}_F} \varphi_{\mathcal{N}}(\xi) exp(\pi i(\xi^2 z_1 + \xi'^2 z_2))$$

is a Hilbert modular form of weight $\frac{1}{2}$ *possibly with a character.*

Proof:

This is a corollary of the Theorem on pg.154 from [Garrett].

Now we prove the key inclusion

$$H \subseteq \Theta$$

Let $\mathbf{A}_f$ denote the finite adeles of F. It is known that (cf. [Del], pg. 259) the metaplectic 2-covering $\widetilde{SL}_2(\mathbf{A}_f)$ of $SL_2(\mathbf{A}_f)$ acts on H, preserves the scalar product and leaves Θ stable.

Under this action, H decomposes into a direct sum of irreducible representations. Let H_i be one of them. We want to prove that H_i is contained in Θ.

Proposition 1. *For suitable* $(\mathcal{N}, \chi)$, $H_i \cap \mathcal{M}_{\frac{1}{2}}(\mathcal{N}, \chi) \neq 0$.

Proof:

There exists a family of compact open subgroups $\{\mathcal{K}_0(\mathcal{N})\}_{\mathcal{N}}$, which is also a fundamental system of neighborhoods of the unity of $\widetilde{SL_2(\mathbf{A_f})}$, such that $\Gamma_0(\mathcal{N}) = \mathcal{K}_0(\mathcal{N}) \cap SL_2(\mathbf{A}_f)$, $\forall \mathcal{N}$. Here we have used the fact that F has class number 1. There is a character $\tilde{\chi}$ whose restriction to $\Gamma_0(\mathcal{N})$ is χ. If V is a vector space on which $\widetilde{SL_2(\mathbf{A_f})}$ acts, we write $V^{\mathcal{K}_0(\mathcal{N}),\tilde{\chi}}$ for the subgroup of vectors $v \in V$ such that $kv = \tilde{\chi}(k)v$. One knows

$$H^{\mathcal{K}_0(\mathcal{N}),\tilde{\chi}} = \mathcal{M}_{\frac{1}{2}}(\mathcal{N}, \chi)$$

We have

$$H^{\mathcal{K}_0(\mathcal{N}),\tilde{\chi}} = \oplus_i H_i^{\mathcal{K}_0(\mathcal{N}),\tilde{\chi}}$$

Now fix any H_i. Then the admissibility of H_i as an $\widetilde{SL_2(\mathbf{A_f})}$-module implies that there exists $(\mathcal{N}, \tilde{\chi})$ such that $H_i^{\mathcal{K}_0(\mathcal{N}),\tilde{\chi}} \neq 0$. Therefore there exists $(\mathcal{N}, \chi)$ such that $H_i \cap \mathcal{M}_{\frac{1}{2}}(\mathcal{N}, \chi) \neq 0$.

QED

One knows that for every prime ideal P of $\mathcal{O}_F$, including those dividing $\mathcal{N}$, there is a Hecke operator $T(P^2)$ acting on $M_{\frac{1}{2}}(\mathcal{N}, \chi)$. They come

from the action of $SL_2(\mathbf{A}_f)$. If P, Q are primes, then $T(P^2)$ commute with $T(Q^2)$. The operators $T(P^2)$ preserve the scalar product and have a common eigenvector in $\mathcal{M}_{\frac{1}{2}}(\mathcal{N}, \chi)$.

Proposition 2.

We have :

$$f(z) = \Sigma_{\mu \in \mathcal{O}_{\mathbf{F}}} a(t\mu^2) exp(t\pi i(\mu^2 z_1 + \mu^{'2} z_2))$$

where $t \in \mathcal{O}_F, t$ is totally positive, $t | \mathcal{N}$, and, $\forall \alpha \in \mathcal{O}_F$,

$$a(\alpha\mu^2) = a(\alpha)\psi(\mu) \text{ if } (\mu, \mathcal{N}) = 1$$

$$a(\alpha P^2) = c_P a(\alpha) \text{ if } P \mid \mathcal{N}$$

where ψ is a multplicative character mod $2\mathcal{N}$ and $T(P^2)f = c_P f$.

Proof:

This is a consequence of the following lemmas:

Lemma 1. *We have*

(i) There is a basis of $\mathcal{M}_{\frac{1}{2}}(\mathcal{N}, \chi)$ consisting of forms whose coefficients belong to a number field,

(ii) If $f(z) = \sum_{\xi \in \mathcal{O}_F} a(\xi) exp(\pi i(\xi^2 z_1 + \xi'^2 z_2))$ belongs to $\mathcal{M}_{\frac{1}{2}}(\mathcal{N}, \chi)$ and the $a(\xi)$ are algebraic numbers then the $a(\xi)$ have bounded denominators (i.e., there exists a nonzero integer D such that $Da(\xi)$ is an algebraic integer for all ξ).

Proof of Lemma 1:

The analogous results for integral weight forms are known. Also it is known that there is an orthogonal decomposition $\mathcal{M}_{\frac{1}{2}}(\mathcal{N}, \chi) = \mathcal{S}_{\frac{1}{2}}(\mathcal{N}, \chi) \oplus \mathcal{E}_{\frac{1}{2}}(\mathcal{N}, \chi)$ for the scalar product,where $\mathcal{S}_{\frac{1}{2}}(\mathcal{N}, \chi)$ denotes the space of cusp forms and $\mathcal{E}_{\frac{1}{2}}(\mathcal{N}, \chi)$ denotes the space of Eisenstein forms. In [Shi2] it is proved that there is a basis of $\mathcal{E}_{\frac{1}{2}}(\mathcal{N}, \chi)$ consisting of forms whose coefficients belong to a number field and have bounded denominators. For both (i) and (ii), it suffices to prove the analogous results for $\mathcal{S}_{\frac{1}{2}}(\mathcal{N}, \chi)$. By Prop 5.2, 5.3 from [Shi1], $\mathcal{S}_{\frac{1}{2}}(\mathcal{N}, \chi)$ is spanned by Hecke eigenforms for $T(P^2)$ for almost all P. Write $\mathcal{S}_{\frac{1}{2}}(\mathcal{N}, \chi) = \Theta_0 \oplus \Theta_0^{\perp}$ where Θ_0 is the subspace of $\mathcal{S}_{\frac{1}{2}}(\mathcal{N}, \chi)$ generated by theta series and $\Theta_0^{\perp}$ is the subspace perpendicular to Θ under the scalar product a corollary of the result of this chapter is $\mathcal{S}_{\frac{1}{2}}(\mathcal{N}, \chi) = \Theta_0$ but we don't know it yet. The analogous

statements of (i) and (ii) hold for Θ_0 by the explicit knowledge of theta series. If $\mathcal{S}_{\frac{1}{2}}(\mathcal{N},\chi) = \Theta_0$ then we are done. If not, then there exists a Hecke eigenform f in $\Theta_0^{\perp}$. As in [Shi1], pg. 816, we associate to f an integral weight form h. It may happen that different f's correspond to the same h. We denote by $\mathcal{S}_{\frac{1}{2}}(\mathcal{N},h,\chi)$ the subspace of $\mathcal{S}_{\frac{1}{2}}(\mathcal{N},\chi)$ generated by those f's corresponding to h. By prop 8.9(2) of [Shi1], $\mathcal{S}_{\frac{1}{2}}(\mathcal{N},h,\chi)$ has a basis of forms whose coefficients belong to a number field and have bounded denominators.

QED

Lemma 2. *Let* $f(z) = \sum_{\xi\in\mathcal{O}_F} a(\xi)exp(\pi i(\xi^2 z_1 + \xi'^2 z_2))$ *be a nonzero element of* $\mathcal{M}_{\frac{1}{2}}(\mathcal{N},\chi)$ *and let* P *be a prime with* $P \not| \mathcal{N}$. *Put* $P = \varpi\mathcal{O}_F$. *Assume that* $f \mid T(P^2) = c_P f$, *with* $c_P \in \mathbf{C}$. *Let* $\mu \in \mathcal{O}_F$ *such that* $P^2 \not| \mu$. *Then:*

(i) $a(\mu P^{2n}) = a(\mu)\chi(\varpi)^n(\frac{\mu}{P})^n$ for every $n \geq 0$ integer,

(ii) If $a(\mu) \neq 0$ then $P \not| \mu$ and $c_P = \chi(\varpi)(\frac{\mu}{P})(1 + \frac{1}{N(P)})$.

Proof of Lemma 2:

Cf. **Prop5.4** pg. 788 in [Shi], the operator $T(P^2)$ maps forms with

algebraic coefficients into themselves. Hence c_P is algebraic and we may assume that the coefficients $a(\xi)$ of f are algebraic numbers. Fix μ and consider the power series

$$A(T) = \sum_{n=0}^{\infty} a(\mu P^{2n}) T^n$$

where T is an indeterminate. As in the proof of **Theorem 5.5**, pg. 790 [Shi] we have

$$A(T) = a(\mu) \frac{1 - \alpha T}{(1 - \beta T)(1 - \gamma T)}$$

where $\alpha = \chi(p) N(P)^{-1} (\frac{\mu}{P})$ and $\beta + \gamma = c_P$, $\beta\gamma = \chi(\varpi^2) N(P)^{-1}$.

If $a(\mu) = 0$ then $A(T) = 0$ thus $a(\mu P^{2n}) = 0$ for all $n \geq 0$ therefore (i).

Assume now $a(\mu) \neq 0$. Using Lemma 1(ii), $A(T)$ converges in the P-adic topology, if we view $A(T)$ as a nonzero P-adic rational function of T, in the P-adic unit disc U defined by $\mid T \mid_P < 1$; hence $A(T)$ cannot have a pole in U. However, since $\beta\gamma = \chi(\varpi^2) P^{-1}$, either β^{-1} or γ^{-1} belongs to U; assume it is β^{-1}. Now $A(T)$ holomorphic at β^{-1} implies that the factors $1 - \beta T$ and $1 - \alpha T$ cancel each other. Thus $\alpha = \beta$ and

$$A(T) = \frac{a(\mu)}{(1 - \gamma T)}$$

thus

$$a(\mu P^{2n}) = \gamma^n a(\mu)$$

Now $\beta\gamma \neq 0 \Rightarrow \alpha \neq 0 \Rightarrow \varpi \not| \mu$. Moreover,

$$\gamma = \frac{\beta\gamma}{\alpha} = \frac{\chi(\varpi^2)N(P)^{-1}}{\chi(\varpi)N(P)^{-1}(\frac{\mu}{\varpi})} = \chi(\varpi)(\frac{\mu}{\varpi})$$

which implies (i). Finally, (ii) follows from $c_P = \beta + \gamma = \alpha + \gamma$.

QED

Lemma 3. *Let* $f(z) = \sum_{\xi \in \mathcal{O}_F} a(\xi) exp(\pi i(\xi^2 z_1 + \xi'^2 z_2))$ *be a nonzero element of* $\mathcal{M}_{\frac{1}{2}}(\Gamma_0(\mathcal{N}, \chi))$ *and let* $\mathcal{N}'$ *be a multiple of* $\mathcal{N}$. *Assume that, for all* $P \not| \mathcal{N}'$, *we have* $f \mid T(P^2) = c_P f$, *with* $c_P \in \mathbf{C}$. *Then there exists a unique (up to multiplication by a unit) square-free nonzero* $t \in \mathcal{O}_F$ *such that* $a(\xi) = 0$ *if* $\frac{\xi}{t}$ *is not a square in* $\mathcal{O}_F$. *Moreover:*

(i) $t \mid \mathcal{N}'$,

(ii) $c_P = \chi(\varpi)(\frac{t}{\varpi})(1 + \frac{1}{N(P)})$ if $\varpi \not| \mathcal{N}'$,

(iii) $a(\xi\mu^2) = a(\xi)\chi(\mu)(\frac{t}{\mu})$ if $(\mu, \mathcal{N})' = 1$.

Proof of Lemma 3:

Let $\mu, \mu' \in \mathcal{O}_F$ such that $a(\mu) \neq 0$ and $a(\mu') \neq 0$. For each P prime in

$\mathcal{O}_F$, $Pp \not| \mathcal{N}'\mu\mu'$ we have, by Lemma 2(ii),

$$\chi(\varpi)(\frac{\mu}{\varpi})(1+\frac{1}{N(P)}) = c_p = \chi(\varpi)(\frac{\mu'}{\varpi})(1+\frac{1}{N(P)})$$

thus, for all ϖ prime in $\mathcal{O}_F$, $\varpi \not| \mathcal{N}'\mu\mu'$,

$$(\frac{\mu}{\varpi}) = (\frac{\mu'}{\varpi}).$$

This implies, for each prime q dividing μ and not dividing μ', denoting by $v_q(\mu)$ the exponent of q in μ, that

$$(\frac{q^{v_q(\mu)}}{\varpi}) = 1$$

for all ϖ prime in $\mathcal{O}_F$, $\varpi \not| \mathcal{N}'\mu\mu'$. In particular, for a ϖ large enough, this implies that $v_q(\mu)$ is even. Therefore we may write $\mu = t\mu_1^2$, $\mu' = t\mu_1'^2$ with t square free. The uniqueness of t follows repeating the argument for another pair μ, μ'' instead of μ, μ'. We proved the first part of the Lemma 3. Now we prove (i) and (ii). Fix a prime p not dividing $\mathcal{N}'$. Fix μ such that $a(\mu) \neq 0$ and write $\mu = t\mu_1^2 = t\varpi^{2n}\mu_0^2$ with ϖ not dividing μ_0. We apply Lemma 2(i) to $t\mu_0^2$ and we get $a(\mu) = a(t\mu_0^2)\chi(\varpi)(\frac{t}{\varpi})(1+\frac{1}{N(P)})$ thus $a(t\mu_0^2) \neq 0$. By Lemma 2(ii), ϖ does not divide $t\mu_0^2$ hence ϖ does not divide t. So

far Lemma 3(i) proved. Now, by Lemma 2(ii), $c_P = \chi(\varpi)(\frac{t}{\varpi})(1 + \frac{1}{N(P)})$ thus Lemma 3(ii) proved. Now we prove Lemma 3(iii). Because both sides are multiplicative in μ, it suffices to check it for $\mu = \varpi$ with ϖ prime not dividing $\mathcal{N}'$. Writing $\xi = \xi_0 \varpi^{2n}$ with $\varpi^2 \not| \mathcal{N}$ and applying Lemma 2(i) we get qed.

QED

Lemma 4. *We have* $a(\mu\varpi^2) = c_P a(\mu)$ *if* $\varpi \mid \mathcal{N}$.

Proof of Lemma 4:

It is a straightforward corollary of [Shi], p.788, **Prop 5.4.**

Consider now

$$g(z) = \Sigma_{\xi \in \mathcal{O}_F, (\xi, \mathcal{N})=1} a(t\xi^2) exp(t\pi i(\xi^2 z_1 + \xi'^2 z_2))$$

Proposition 3.

(i) $g \neq 0$;

(ii) $g \in \Theta$;

(iii) g is (up to a scalar factor) the transform of

$$f(z) = \Sigma_{\xi \in \mathcal{O}_F} a(t\xi^2) exp(t\pi i(\xi^2 z_1 + \xi'^2 z_2))$$

by $\Pi_{P|\mathcal{N}} L_P$ where $P = \varpi\mathcal{O}_F$ with ϖ totally positive and L_P is the operator which transforms $h(z)$ into $h(z) - c_P h(\varpi^2 z_1, \varpi'^2 z_2)$.

(iv) L_p can be defined by the element

$$1 - c_P \begin{pmatrix} \varpi^{-1} & 0 \\ 0 & \varpi \end{pmatrix}$$

of the group ring $\mathbf{Z}[\widetilde{SL_2}(F_P)]$, where F_P is the completion of F at P.

(v) $g \in H_i$.

Proof:

(i)$g \neq 0$ because $f \neq 0$;

(ii) Define $\varphi_{\mathcal{N}}(\xi) = a(t\xi^2)$ if $(\xi, \mathcal{N}) = 1$ and $\varphi_{\mathcal{N}}(\xi) = 0$ otherwise. φ is periodic of period $\mathcal{N}$ because ψ is so. Therefore

$$g(z) = \Sigma_{\xi \in \mathcal{O}_F} \varphi_{\mathcal{N}}(\xi) exp(t\pi i(\xi^2 z_1 + \xi'^2 z_2)) \in \Theta.$$

(iii) Fix $P = \varpi\mathcal{O}_F \mid \mathcal{N}$ with ϖ totally positive. We have

$$(L_P f)(z) = \Sigma_{\xi \in \mathcal{O}_F} a(t\xi^2) exp(t\pi i(\xi^2 z_1 + \xi'^2 z_2)) -$$

$$c_p \Sigma_{\xi \in \mathcal{O}_F} a(t\xi^2) exp(t\pi i(\xi^2 \varpi^2 z_1 + \xi'^2 \varpi'^2 z_2)) =$$

$$\Sigma_{\xi \in \mathcal{O}_F} a(t\xi^2) exp(t\pi i(\xi^2 z_1 + \xi'^2 z_2)) -$$

$$\Sigma_{\xi\in\mathcal{O}_F} a(t(\varpi\xi)^2) exp(t\pi i(\xi^2\varpi^2 z_1 + \xi'^2\varpi'^2 z_2)) =$$

$$\Sigma_{\xi\in\mathcal{O}_F,(\xi,\varpi)=1} a(t\xi^2) exp(t\pi i(\xi^2 z_1 + \xi'^2 z_2))$$

in other words L_P "deletes" from the expansion of f those terms such that $\varpi \mid \xi$. The conclusion follows noticing that $\Pi_{P|N} L_P$ means composition of operators.

(iv)

$SL_2(F)$ embeds diagonally in $\widetilde{SL}_2(\mathbf{A}) = \widetilde{SL}_2(F_\infty) \times \widetilde{SL}_2(\mathbf{A}_f)$ with componentwise multiplication. Write the elements of $\widetilde{SL}_2(\mathbf{A})$ as (x_∞, x_f) with $x_\infty \in \widetilde{SL}_2(F_\infty)$ and $x_f \in \widetilde{SL}_2(\mathbf{A}_f)$. If $\gamma \in SL_2(F)$ then $\gamma_\infty = \gamma$ $\gamma_f = \gamma$ and $\gamma := (\gamma, \gamma) = (\gamma, 1)(1, \gamma)$.

Let $\gamma = \begin{pmatrix} \varpi^{-1} & 0 \\ 0 & \varpi \end{pmatrix} \in SL_2(F)$. Also note that $\begin{pmatrix} \varpi^{-1} & 0 \\ 0 & \varpi \end{pmatrix} \in \widetilde{SL}_2(F_P) \subseteq \widetilde{SL}_2(\mathbf{A}_f)$. Since the automorphic forms are left invariant under the diagonal action of $SL_2(F)$, the action of γ in $\widetilde{SL_2}(\mathbf{A}_f)$ is the inverse of the action of $(\gamma, 1)$. By part (iii), $\gamma \in \widetilde{SL}_2(\mathbf{A}_f)$ sends $h(z)$ to $h(\varpi^2 z_1, \varpi'^2 z_2)$. Since $L_P(h)(z) = h(z_1, z_2) - c_P h(\varpi^2 z_1, \varpi'^2 z_2)$, the conclusion follows.

(v) follows from (iii),(iv) and the fact that H_i is invariant.

Therefore $H_i \cap \Theta \neq \emptyset$. Since H_i is irreducible, this implies $H_i \subseteq \Theta$.

QED

Chapter 4

Examples

Consider $F = \mathbf{Q}[\sqrt{2}]$ and $\mathcal{N} = 8\mathbf{Z}[\sqrt{2}]$.

From the proofs in Chapter 4 follows that $\sum_\chi \mathcal{M}_{\frac{1}{2}}(2^n\mathbf{Z}[\sqrt{2}], \chi)$ is generated by $\{(g_\psi)_t\}$ where ψ is an even primitive character modulo $\mathcal{N}$ and t is a totally positive integer of F dividing 2.

The coset representatives of $\mathcal{O}_F/\mathcal{N}$ are $\{a + b\sqrt{2} + \mathcal{N}\}$ with $a, b \in \{0, ..., 7\}$ so that $\mathcal{O}_F/\mathcal{N}$ has 64 elements. For $\alpha = a + b\sqrt{2}$, we denote $[\alpha] := a + b\sqrt{2} + \mathcal{N}$. Since $\mathcal{O}_F/\mathcal{N}$ is finite, the elements of $(\mathcal{O}_F/\mathcal{N})^*$ are exactly the nonzero divisors. Notice that $[a + b\sqrt{2}]$ is a zero divisor in $\mathcal{O}_F/\mathcal{N}$ if and only if a is even. Thus $(\mathcal{O}_F/\mathcal{N})^*$ has 32 elements. We list the orders of all elements (and we conclude that $(\mathcal{O}_F/\mathcal{N})^*$ has exponent 8):

$[3], [5], [7]$ and $[a + 4\sqrt{2}]$, a odd, have order 2;

$[a + 2\sqrt{2}], [a + 6\sqrt{2}]$, a odd, have order 4;

$[a + b\sqrt{2}]$, a, b odd, has order 8.

Thus, counting the elements of order 2 in an abelian group of order

32 and exponent 8, we conclude that $(\mathcal{O}_F/\mathcal{N})^* \cong \mathbf{Z}/8 \times \mathbf{Z}/2 \times \mathbf{Z}/2$ since they have the same maximum number of 7 elements of order 2. Any other abelian group of order 32 and exponent 8 has less than 7 elements of order 2.

It is straightforward to check that $[1+\sqrt{2}]$ generates a subgroup of order 8, that $[-1] = [7]$ generates a subgroup of order 2, that $[3+4\sqrt{2}]$ generates a subgroup of order 2, that $[7] \notin < [1+\sqrt{2}] >$, and that $[3+4\sqrt{2}] \notin < [7] > \times < [1+\sqrt{2}] >$. It follows that $(\mathcal{O}_F/\mathcal{N})^* = < [1+\sqrt{2}] > \times < [7] > \times < [3+4\sqrt{2}] >$. The character group of (the finite abelian group) $(\mathcal{O}_F/\mathcal{N})^*$ is therefore $< \varphi_0 > \times < \varphi_1 > \times < \varphi_2 >$ where

$< \varphi_0 > \equiv 1$ on $< [7] > \times < [3+4\sqrt{2}] >$, hence $< \varphi_0 >$ can be viewed as a character of $< [1+\sqrt{2}] >$;

$< \varphi_1 > \equiv 1$ on $< [1+\sqrt{2}] > \times < [3+4\sqrt{2}] >$, hence $< \varphi_1 >$ can be viewed as a character of $< [7] >$;

$< \varphi_2 > \equiv 1$ on $< [7] > \times < [1+\sqrt{2}] >$, hence $< \varphi_2 >$ can be viewed as a character of $< [3+4\sqrt{2}] >$.

Any character ψ of $(\mathcal{O}_F/\mathcal{N})^*$ can be written as $\psi = \varphi_0^{j_0}\varphi_1^{j_1}\varphi_2^{j_2}$ with

$j_0 \in \{0, ..., 7\}$, $j_1 \in \{0, 1\}$, $j_2 \in \{0, 1\}$. Recall that all the units of $\mathcal{O}_F$ are $\{\pm(1+\sqrt{2})^k,\ k \in \mathbf{Z}\}$, so that ψ is even if and only if $\psi \equiv 1$ on $< [7] > \times < [1+\sqrt{2}] >$, that is $j_0 = 0$ and $j_1 = 0$, therefore all the even characters of $(\mathcal{O}_F/\mathcal{N})^*$ are $\{1, \psi := \varphi_2\}$.

So far we got that $\{\theta, \theta_\psi, \theta_2, (\theta_\psi)_2, \theta_{\sqrt{2}}, (\theta_\psi)_{\sqrt{2}}\}$ is a set of generators for $\sum_\chi \mathcal{M}_{\frac{1}{2}}(8\mathbf{Z}[\sqrt{2}], \chi)$. Since these six generators have six distinct characters, we conclude:

$\{\theta\}$ is a basis for $\mathcal{M}_{\frac{1}{2}}(4\mathbf{Z}[\sqrt{2}])$;

$\{\theta_\psi\}$ is a basis for $\mathcal{M}_{\frac{1}{2}}(4\mathbf{Z}[\sqrt{2}], \psi)$;

$\{\theta_{\sqrt{2}}\}$ is a basis for $\mathcal{M}_{\frac{1}{2}}(4\sqrt{2}\mathbf{Z}[\sqrt{2}], \chi_{\sqrt{2}})$;

$\{(\theta_\psi)_{\sqrt{2}}\}$ is a basis for $\mathcal{M}_{\frac{1}{2}}(4\sqrt{2}\mathbf{Z}[\sqrt{2}], \psi\chi_{\sqrt{2}})$;

$\{\theta_2\}$ is a basis for $\mathcal{M}_{\frac{1}{2}}(8\mathbf{Z}[\sqrt{2}], \chi_2)$;

$\{(\theta_\psi)_2\}$ is a basis for $\mathcal{M}_{\frac{1}{2}}(8\mathbf{Z}[\sqrt{2}], \psi\chi_2)$.

A generalization is :

$\mathcal{O}_F = \mathbf{Z}[\sqrt{2}]$, $\mathcal{N} = 2^n\mathbf{Z}[\sqrt{2}]$, $n \in \mathbf{Z}, n \geq 4$

With similar arguments we get that :

$(\mathcal{O}_F/\mathcal{N})^*$ has 2^{2n-1} elements and has exponent 2^n;

All the elements of the form $[a+b\sqrt{2}]$ of order two are a, $a \neq 1$ odd (there are $2^{n-1}-1$ of them) and $[a+2^{n-1}\sqrt{2}]$, a odd (there are 2^{n-1} of them).

All the elements of order 2^n are $[a+b\sqrt{2}]$ with a, b odd.

Counting the elements of order 2, we conclude $(\mathcal{O}_F/\mathcal{N})^* \cong \mathbf{Z}/2^n \times \prod_{j=1}^{n-1} \mathbf{Z}/2$. Its group of characters is generated by φ_0 of order 2^n and $\varphi_1, ..., \varphi_{n-1}$ each of order 2. Without loss of generality $\varphi_1 \equiv 1$ on $< [-1] >$. Any even characters ψ can be written as $\varphi_2^{j_2} .... \varphi_{n-1}^{j_{n-1}}$ with $j_2, ..., j_{n-1} \in \{0,1\}$.

Proposition.

A basis for $\sum_\chi \mathcal{M}_{\frac{1}{2}}(2^n\mathbf{Z}[\sqrt{2}], \chi)$ is given by

$$\{(\theta_\psi)_t,\ \psi = \varphi_2^{j_2} .... \varphi_{n-1}^{j_{n-1}}\ ,\ j_2, ..., j_{n-1} \in \{0,1\}\ ,\ t \mid 2^{n-2}, t > 0\}.$$

Remark.

A character on $\mathcal{O}_F$ is the pull-back of a character on $\mathbf{Z}$ via norm iff it is invariant under the Galois action. For $\mathcal{N} = 8\mathbf{Z}[\sqrt{2}]$, the forms θ and θ_ψ

have such characters, since every element of order 2 in $(\mathcal{O}_F/\mathcal{N})^*$ is invariant under the Galois action. However, the forms $\{(\theta_\psi)_{\sqrt{2}}, \theta_{\sqrt{2}}\}$ are genuinely new.

Chapter 5

Towards the congruent number problem over F

Let F be a totally real number field. Below $\alpha \in F$ and $\tau : F \to \mathbf{R}$ denotes a field embedding.

Definitions:

(i) $x \in F$ is said to be τ**-positive** iff $\tau(x) > 0$;

(ii) $x \in F$ is said to be **totally positive** iff $\tau(x) > 0\,, \forall \tau$

(iii) $\alpha \in F$ is said to be an F**-congruent number with respect to** τ iff

$$\exists \tau - \text{positive}\, X, Y, Z \,\text{such that}\, X^2 + Y^2 = Z^2 \,\text{and}\, \frac{1}{2}\tau(X)\tau(Y) = \tau(\alpha)$$

Note that an F-congruent number with respect to τ is τ-positive. Also, note that by applying τ^{-1} the last equality becomes

$$\frac{1}{2}XY = \alpha$$

(iv) $\alpha \in F$ is said to be an F**-congruent number for all** τ iff α is an F-congruent number with respect to $\tau, \forall \tau$.

Our goal is to generalize the concept of $\mathbf{Q}$-congruent number to F-congruent number and give criteria for α to be an F-congruent number. Note that there are two generalizations: "F-congruent number with respect to a (fixed) τ" and "F-congruent number $\forall\tau$." These are distinct as as the following example shows:

Example

Let $F = \mathbf{Q}$, $\alpha = 78 + 58\sqrt{2}$, $X = 3 + 4\sqrt{2}$, $Y = 20 + 12\sqrt{2}$, $Z = 21 + 12\sqrt{2}$, $\tau(a + b\sqrt{2}) = a + b\sqrt{2}$ and observe that α is an F-congruent number with respect to τ but α is not totally positive.

Important: From now on we fix a τ and by "positive" we mean "τ-positive" and by "F-congruent number" we mean "F-congruent number with respect to τ."

Problem: Find criteria for α to be an F-congruent number.

Proposition 1. *$\alpha \in F$ is an F-congruent number $\Rightarrow$ $\forall x \in F$, $x^2\alpha$ is an F-congruent number.*

Proof.

By definition, $\exists X, Y, Z > 0$ such that $X^2 + Y^2 = Z^2$ and $XY = 2\alpha$. Multiplying both equalities by x^2 we get that $x^2\alpha$ is an F-congruent number corresponding to the triple xX, xY, xZ by choosing $x > 0$.

Define an equivalence relation as follows:

$$\alpha_1 \sim \alpha_2 \Leftrightarrow \exists x \in F^* \,\text{such that}\, \alpha_1 = x^2\alpha_2$$

Definition. *$\alpha \in \mathcal{O}_F$ is said to be* **square free** *iff $\nexists P$ prime ideal in $\mathcal{O}_F$ such that $P^2 \mid (\alpha)$.*

In particular, any unit of $\mathcal{O}_F$ is square free.

Proposition 2.

$$\forall \alpha \in F\,,\, \alpha > 0\,,\, \exists \alpha_0 \in \mathcal{O}_F\,,\, \alpha_0 > 0 \,\text{such that}\, \alpha \sim \alpha_0$$

Proof.

Multiply α by the square of its denominator.

Important: From now on when we want to find out if $\alpha \in F\,,\, \alpha > 0$ is an F-congruent number we may assume that $\alpha \in \mathcal{O}_F\,,\, \alpha > 0$ and square free.

Lemma 1. *Let E_α be the elliptic curve $y^2 = x^3 - \alpha^2 x$. All the points of $E_\alpha(F)$ of order 2 are*

$$\{(0,0),(\alpha,0),(-\alpha,0)\}$$

Proof.

Let $O \neq P = (x_P, y_P) \in E_\alpha(F)$, $2P = O$. Cf. [Kob],pg.34 $x_{2P} = (\frac{x_P^2+\alpha^2}{2y_P})^2$ thus $2P = O \Rightarrow y_P = 0 \Rightarrow x_P^3 - \alpha^2 x_P = 0 \Rightarrow x_P \in \{0, \pm\alpha\}$. Conversely any $(x,0) \in E_\alpha(F)$ has order two.

QED

Proposition 3. *Let E_α be the elliptic curve $y^2 = x^3 - \alpha^2 x$. If $\exists P \in E_\alpha(F)$ such that $2P \neq O$ then α is an F-congruent number.*

Proof.

Replacing P by $2P$ we may assume that $P = (x,y)$ with x a square in F, in particular $x > 0$. Because $2P \neq 0$, we have that $y \neq 0$. Indeed, assuming by contradiction $y = 0$, we get, from $y^2 = x^3 - \alpha^2 x$, that $P = (x,y) \in \{(0,0),(\alpha,0),(-\alpha,0)\}$ which are elements of order two in $E_\alpha(F)$. Eventually replacing $P = (x,y)$ by $-P = (x,-y)$ we may assume that

$y > 0$.

Let $X = \frac{(x+\alpha)(x-\alpha)}{y}$, $Y = 2\alpha\frac{x}{y}$. Note that $XY = 2\alpha$ and $X^2 + Y^2 = (\frac{(x^2+\alpha^2)}{y})^2$. We have that $Y > 0$. Also $X > 0$ from $XY = 2\alpha$. Taking $Z = \frac{(x^2+\alpha^2)}{y} > 0$ we get a triple $X, Y, Z > 0$ defining α to be an F-congruent number.

QED

Fix $\alpha \in F^*$.

Proposition 4. *If $F/\mathbf{Q}$ Galois then*

$$\varphi(\mid E_\alpha(F)_{tors} \mid) \leq 2[F : \mathbf{Q}]$$

where φ denotes the totient Euler function.

Proof.

Denote $K = \mathbf{Q}(i)$. Let d be the density function as defined in $[Neuk]$. Let $Y = \{(p)$ prime ideal of $\mathbf{Z}$ such that $p \equiv 3(mod\, 4)$ and p splits completely in $\mathcal{O}_F\}$. We have that $F \cap K = \mathbf{Q} \Rightarrow d(Y) = \frac{1}{2}\frac{1}{[F:\mathbf{Q}]}$ using [Neuk], cor(13.6)pg547. Let $m =\mid E_\alpha(F)_{tors} \mid$.

Claim

$$m \mid p+1\,,\ \forall (p) \in Y \text{ but finitely many}$$

Proof of Claim

Here we denote points on the elliptic curve with projective coordinates, (x, y, z) satisfying $y^2z = x^3 - n^2xz^2$ so that we may assume $E_\alpha(F)_{tors} = E_\alpha(\mathcal{O}_F)_{tors}$.

For any prime ideal $P \in \mathcal{O}_F$ we define the "reduction mod P" map

$$\varphi_P : E_\alpha(F)_{tors} = E_\alpha(\mathcal{O}_F)_{tors} \to E_\alpha(\mathcal{O}_F/P)_{tors}$$

$$(x, y, z) \mapsto (\bar{x}, \bar{y}, \bar{z})$$

For every $(p) \in Y$ fix P ideal of $\mathcal{O}_F$ dividing $p\mathcal{O}_F$ and denote $\varphi_p = \varphi_P$. Because p splits completely in $\mathcal{O}_F$ we have that $\mathcal{O}_F/P = \mathbf{F}_p$. From [Kob] page 40 we get $\mid E_\alpha(\mathbf{F}_p)_{tors} \mid = p+1$ (here we use $p \equiv -1 (mod\, 4)$). Finally, for all but finitely many $(p) \in Y$ we have that φ_p is injective, by using a similar argument to that one in [Kob] pp 44-45: first we notice that $(\bar{x}_1, \bar{y}_1, \bar{z}_1) = (\bar{x}_2, \bar{y}_2, \bar{z}_2)$ iff P divides the $gcd(y_1z_2 - y_2z_1, x_2z_1 - x_1z_2, x_1y_2 - y_2x_1)$ then, because only finitely many P's divide this gcd, we conclude that φ_p is injective for all but finitely many p's.

We proved the claim, that is

$$p \equiv -1(mod\, m)\ ,\ \forall(p) \in Y \text{ but finitely many}$$

Let $A = \{p \in \mathbf{Z}\ ,\ p \equiv -1(mod\, m)\}$. We have $d(A) \geq d(Y) = \frac{1}{2}\frac{1}{[F:\mathbf{Q}]}$. On the other hand Dirichlet density theorem (cf. [Neuk] pg.54) implies that $d(A) = \frac{1}{\varphi(m)}$.

QED.

Corollary 1. *If* $[F : \mathbf{Q}] = 2$ *then*

$$\mid E_\alpha(F)_{tors} \mid \in \{4, 8, 12\}$$

Proof.

It follows from Proposition 4 and Lemma 1.

Proposition 5. *If* $[F : \mathbf{Q}] = 2$ *and* α *is not a square in* F *then*

$$\mid E_\alpha(F)_{tors} \mid \neq 8$$

Proof.

By contradiction; assume, via Lemma1, that $\exists P = (x, y) \in E_\alpha(F)_{tors}$ of order four. Then $2P$ has order two thus $y_{2P} = 0$ and $x_{2P} = (\frac{x_P^2+\alpha^2}{2y_P})^2 \in \{0, \pm\alpha\}$ that is it is equal to α thus α is a square in F, contradiction.

QED

Proposition 6. 3 *does not divide* $\mid E_\alpha(F)_{tors} \mid$.

Proof.

In our case we know that 3 is inert in $K = \mathbf{Q}[i]$ so the associated elliptic curve is supersingular there. Looking at the representation of G_F on $E[3]$ one has the following possibilities:

(i) 3 is inert in F, in which case the representation is irreducible;

(ii) 3 splits in F, in which case the representation splits as $\chi \oplus \chi$ with χ a non-trivial character of G_F.

Consequently, no vector (other than zero) in $E[3]$ is fixed by G_F , and so there is no nonzero point of order 3 in $E(F)$.

QED

Corollary 2. *If* $[F : \mathbf{Q}] = 2$ *and* α *is not a square in* F *then*

$$\mid E_\alpha(F)_{tors} \mid = 4$$

Proof.

It follows from Cor 1, Prop 5 and Prop 6.

Lemma2. *$\exists$ a bijection between*

$$S := \{0 < X < Y < Z \in F\,,\, X^2 + Y^2 = Z^2\,,\, \frac{1}{2}XY = \alpha\}$$

and

$$T := \{x \in F^*\,,\, x, x+\alpha, x-\alpha \in F^2\}$$

Proof.

The following two functions

$$S \longrightarrow T$$

$$(X, Y, Z) \mapsto x = (\frac{Z}{2})^2$$

and

$$T \longrightarrow S$$

$$x \mapsto (X = \sqrt{x+\alpha} - \sqrt{x-\alpha}, Y = \sqrt{x+\alpha} + \sqrt{x-\alpha}, Z = 2\sqrt{x})$$

are inverse each other.

QED

Proposition 7. *If $[F : \mathbf{Q}] = 2$ and α is not a square in $\mathcal{O}_F$ TFAE:*

(i) $\exists P \in E_\alpha(F)$ such that P has infinite order;

(ii)$\exists P \in E_\alpha(F)$ such that $2P \neq O$;

(iii)α is an F-congruent number.

Proof.

(i)$\Rightarrow$ (ii) trivial;

(ii)$\Rightarrow$(iii) see Proposition 3;

(iii)$\Rightarrow$(i) for this implication only we need the hypothesis $[F : \mathbf{Q}] = 2$ and α is not a square in $\mathcal{O}_F$. If α is an F-congruent number then by Lemma2 $\exists x \in F^*$ such that $y := \sqrt{x(x+\alpha)(x-\alpha)} \in F$ that is $(x, y) \in E_\alpha(F)$. We claim that (x, y) has infinite order in $E_\alpha(F)$. Assume it doesn't, then $(x, y) \in E_\alpha(F)_{tors}$ which by Cor2 and Lemma1 is $\{O, (0, 0), (\alpha, 0), (-\alpha, 0)\}$. Because $(x, y) \neq O$, it follows that $y = 0$ and $x \in \{0, \pm\alpha\}$ but $x \in F^* \cap F^2$ thus $\alpha = x$ is a square, contradiction.

QED

Bibliography

[Del] P. Deligne, *Sommes de Gauss Cubiques et Revetements de SL(2), d'apres S. J. Patterson*, In: Lecture Notes in Mathematics, 770, pp. 244-277, Springer, 1980.

[Garret] P. B. Garret, *Holomorphic Hilbert Modular Forms*, Wadsworth & Brooks/Cole Mathematics Series, 1990.

[Kob] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer, 1984

[Neuk] J. Neukirch, *Algebraic Number Theory*, Springer, 1999.

[Serre-Stark] J. P. Serre & H. M. Stark, *Modular Forms of weight 1/2*, In: Modular functions of one variableVI. Lecture Notes in Mathematics, vol. 627, pp. 27-68.Berlin Heidelberg New York: Springer 1977.

[Shi] G. Shimura, *On Hilbert Modular Forms of Half-integral Weight*, In: Duke Mathematical Journal, vol. 55, No. 4. December 1987.

[Shi2] G. Shimura, *On Eisenstein Series of Half-Integral Weight*, In: Duke Mathematics Journal, vol. 52, No.2, June 1985

[Tunnel] J. B. Tunnel, *A classical Diophantine Problem and Modu-*

lar Forms of Weight 3/2, In: Inventiones mathematicae 72, pp. 323-334, Springer-Verlag 1983.

[Vas] L. N. Vaserstein *On the Group SL(2) over Dedekind Rings of Arithmetic Type*, In: Math. Sbornik vol. 18, 1972