Some cyclo-quaternionic lattices.

Gabriele Nebe *
Lehrstuhl B für Mathematik, RWTH Aachen
Templergraben 64, D-52062 Aachen

Abstract.
The faithful lattices of rank $2(p-1)$ of the groups $SL_2(p)$ are described. For small primes p these and related lattices are investigated by computer. In particular a new extremal even unimodular lattice of rank 48 is constructed.

Introduction.

The study of finite integral matrix groups is one source for producing nice lattices. In particular representations of the group $PSL_2(p)$ for $p \equiv 3 \pmod 4$ have been studied in [10] in connection with globally irreducible representations. Gross gives an interpretation of some of the invariant lattices as Mordell-Weil lattices. Since the real Schur index of the faithful rational representations of $SL_2(p)$ of degree $2(p-1)$ is two, they can be viewed as representations over totally definite quaternion algebras. The present article grew out of the investigation of finite quaternionic matrix groups [13].

The paper is organized as follows: After introducing notation and general arguments the faithful lattices of degree $2(p-1)$ of $SL_2(p)$ are described. For $p \equiv 1 \pmod 4$ these lattices can be constructed as cyclotomic lattices over quaternion algebras, as described in section 3. In the next section it is shown that some of these lattices coincide with the very dense Mordell-Weil lattices discovered by Elkies and Shioda [23]. The concluding section deals with those $SL_2(p)$-lattices for which the endomorphism ring is a maximal order in the quaternion algebra with center $\mathbb{Q}[\sqrt{p}]$ ramified only at the two infinite places.

This article is written during a fellowship at the university of Bordeaux financed by the Deutsche Forschungsgesellschaft. I am grateful to both organizations. Finally I want to thank K. Belabas for his help in solving problems with PARI.

*e-mail: gabi@math.rwth-aachen.de

1 General notation and properties.

Let $G \leq GL_n(\mathbb{Q})$ - following P. Hall the symbol $\leq$ is used to denote "is subgroup of" - be a finite subgroup of the group of rational invertible $n \times n$ matrices. There are two important sets that describe the G-invariant Euclidean lattices in $\mathbb{Q}^n$: the set

$$\mathcal{L}(G) := \{L \leq \mathbb{Q}^n \mid L \text{ is a full } \mathbb{Z}\text{-lattice in } \mathbb{Q}^n \text{ and } Lg \leq L \text{ for all } g \in G\}$$

of G-invariant lattices and the vector space of G-invariant quadratic forms

$$\mathcal{F}(G) := \{F \in M_n(\mathbb{Q}) \mid F = F^{tr} \text{ and } gFg^{tr} = F \text{ for all } g \in G\}.$$

$\mathcal{F}(G)$ is a subspace of the vector space of the rational symmetric $n \times n$ matrices and contains the non empty subset $\mathcal{F}_{>0}(G)$ consisting of the positive definite invariant quadratic forms. The space $\mathcal{F}(G)$ can be viewed as the space of symmetric homomorphisms from the natural representation $g \mapsto g$ to its contragredient representation $g \mapsto (g^{-1})^{tr}$. Its dimension can be calculated by decomposing the representation over the reals. The representation is irreducible over $\mathbb{R}$ if and only if $\mathsf{dim}_{\mathbb{Q}}(\mathcal{F}(G)) = 1$. In this case the matrix group G is called *uniform*, because then there is up to scalar multiples a unique G-invariant quadratic form.

If $L \in \mathcal{L}(G)$ is a G-invariant lattice and $F \in \mathcal{F}_{>0}(G)$ then the dual lattice

$$L^{\#} := L^{\#,F} := \{v \in \mathbb{Q}^n \mid lFv^{tr} \in \mathbb{Z} \text{ for all } l \in L\}$$

is again G-invariant, i.e. $L^{\#} \in \mathcal{L}(G)$.

Two lattices (L, F) and (L', F') are called *isometric* if there is an *isometry* $T \in GL_n(\mathbb{Q})$ with $LT = L'$ and $TF'T^{tr} = F$. The *automorphism group* $Aut(L, F)$ is the group of all isometries of (L, F) with itself. Isometries of definite lattices in medium-sized dimensions may be calculated using the algorithm described in [18].

(L, F) is called *integral* if $L \subseteq L^{\#}$ and *unimodular* if $L = L^{\#}$. If $p \in \mathbb{N}$, the *rescaled lattice* (L, pF) of the Euclidean lattice (L, F) is denoted by ${}^{(p)}L$. Generalizing the notion of unimodularity, a lattice (L, F) is called *p-modular* if the rescaled dual lattice ${}^{(p)}L^{\#} = (L^{\#}, pF)$ is isometric to (L, F). For primes p (or $p = 1$) with $k_1 := \frac{24}{p+1} \in \mathbb{N}$ it follows from [19] that the *minimum* $\mathsf{min}(L, F) := \mathsf{min}\{l^{tr}Fl \mid 0 \neq l \in L\}$ of an even p-modular lattice (L, F) of dimension n is at most $2[\frac{n}{2k_1}] + 2$. An even p-modular lattice is called *extremal* if its minimum equals $2[\frac{n}{2k_1}] + 2$.

One further measure of the quality of a Euclidean lattice (L, F) is its *Hermite parameter* $\gamma(L, F) := \frac{\mathsf{min}(L,F)}{(\mathsf{det}(L,F))^{1/n}}$ where $\mathsf{det}(L, F)$ is the *determinant* of L

i.e. the determinant of a Gram matrix of L (with respect to F) and $n := \mathsf{dim}(L)$ is the dimension of L. This is related to the density of the lattice.

The lattice (L, F) is said to be *primitive* if the ideal generated by the values of the bilinear form F on L is $\mathbb{Z}$.

In abuse of notation a subgroup $G \leq GL_n(\mathbb{Q})$ is called *irreducible* if the natural representation is irreducible. By Schur's Lemma G is irreducible if and only if the *endomorphism algebra* $End(G) := \{x \in M_n(\mathbb{Q}) \mid xg = gx \text{ for all } g \in G\}$ is a skewfield.

Lemma 1.1 *Let G be an irreducible subgroup of $GL_n(\mathbb{Q})$ and assume that $\mathsf{dim}(\mathcal{F}(G)) \leq 2$. Let $F \in \mathcal{F}_{>0}(G)$, $L \in \mathcal{L}(G)$.*

(i) If G is uniform then $C := End(G)$ is isomorphic to either $\mathbb{Q}$, an imaginary quadratic number field, or a positive definite quaternion algebra with center $\mathbb{Q}$. If $\mathsf{dim}(\mathcal{F}(G)) = 2$ then C is either an abelian number field with maximal real subfield of degree 2 over $\mathbb{Q}$ or a positive definite quaternion algebra over a real quadratic number field. The mapping $x \mapsto xF$ is an isomorphism from the maximal real subfield of the center of C to $\mathcal{F}(G)$.

(ii) The anti-automorphism $\iota : C \to C; x \mapsto Fx^{tr}F^{-1}$ is independent of the choice of $F \in \mathcal{F}_{>0}(G)$. If C is commutative then ι induces the complex conjugation on C. If C is a quaternion algebra then ι is the canonical involution of C.

(iii) If the endomorphism ring *$\mathfrak{M} := End_L(G) := \{x \in C \mid Lx \subseteq L\}$ is stable under the map ι of (ii) then $\mathfrak{M}$ is also the endomorphism ring of the dual lattice $L^{\#,F}$. The condition holds if $\mathfrak{M}$ contains the maximal order of the fixed field of the restriction of ι to the center of C and in particular if G is uniform.*

Proof: (i) Well known (cf. e.g. [14, Remark (II.1)]).
(ii) Let $x \in C$, $g \in G$. Then $g\iota(x)g^{-1} = gFx^{tr}F^{-1}g^{-1} = Fg^{-tr}x^{tr}g^{tr}F^{-1} = \iota(x)$, hence $\iota(x) \in C$. Moreover ι^2 is the identity on C and $\iota(xy) = \iota(y)\iota(x)$ for all $x, y \in C$. Since for any $F' \in \mathcal{F}(G)$ the matrix $F'F^{-1}$ lies in the center of C, the map ι is independent of F. Moreover, $x \in C$ is a fixed point of ι if and only if xF is symmetric. Therefore $\iota(x) = x \Leftrightarrow x$ lies in the maximal real subfield of the center of C. Galois theory resp. [20, Theorem 8.11.2] now implies (ii).
(iii) Let $x \in \mathfrak{M}$, $l \in L$, and $v \in L^{\#}$. Then $lF(vx)^{tr} = lFx^{tr}F^{-1}Fv^{tr} \in \mathbb{Z}$ since $Fx^{tr}F^{-1} = \iota(x) \in \mathfrak{M}$. So $vx \in L^{\#}$ and therefore $\mathfrak{M} \subseteq End_{L^{\#}}(G)$. Equality follows since $L^{\#\#} = L$. Now assume that $\mathfrak{M}$ contains the maximal order of the fixed field of the restriction of ι to the center of C. If C is a quaternion algebra and tr denotes the reduced trace $tr : C \to Z(C)$ then $\iota(x) = tr(x) - x$ for all $x \in C$. Since $tr(\mathfrak{M})$ lies in the maximal order of the fixed field of the

restriction of ι to the center of C, $\mathfrak{M}$ is stable under ι. If C is commutative then similarly $\iota(\mathfrak{M}) = \mathfrak{M}$. If G is uniform, the fixed field of ι is $\mathbb{Q}$ and $\iota(\mathfrak{M}) = \mathfrak{M}$, because $\mathfrak{M}$ contains $\mathbb{Z}$. □

If one has a subalgebra $\mathcal{Q} \subseteq \mathcal{H}$ of a quaternion algebra $\mathcal{H}$, one might ask, what happens with the maximal orders? Clearly, if $\mathfrak{N}$ is a maximal order of $\mathcal{Q}$ then there is a maximal order $\mathfrak{M}$ of $\mathcal{H}$ containing $\mathfrak{N}$.

The case where $\mathcal{Q}$ itself is a quaternion algebra is much easier than the one where $\mathcal{Q}$ is abelian, because then $Z(\mathfrak{M})\mathfrak{N}$ is of finite index in $\mathfrak{M}$.

Restricting oneself to the situation occurring in this paper, one finds:

Proposition 1.2 *Let $1 < p \in \mathbb{N}$ be square-free, $\mathcal{H} \cong \mathcal{Q}_{\sqrt{p},\infty,\infty}$ the totally definite quaternion algebra over $\mathbb{Q}[\sqrt{p}]$ only ramified at the two infinite places, $\mathcal{Q} \subseteq \mathcal{H}$ a quaternion algebra with center $\mathbb{Q}$, and $\mathfrak{N}$ a maximal order of $\mathcal{Q}$.*

There are exactly 2^s different maximal orders of $\mathcal{H}$ containing $\mathfrak{N}$ where s is the number of ramified finite primes of $\mathcal{Q}$ that do not ramify in $\mathbb{Q}[\sqrt{p}]$.

Proof: Let $\mathfrak{M}$ be a maximal order of $\mathcal{H}$ containing $\mathfrak{N}$. Consider $\mathfrak{M}$ as a $\mathfrak{M}-\mathfrak{M}$-bi-lattice. Then the maximal orders of $\mathcal{H}$ that contain $\mathfrak{N}$ are the endomorphism rings $End_L(\mathfrak{M})$ of the $\mathfrak{M}-\mathfrak{N}$-lattices L in $\mathcal{H}$. These lattices L are of the form $\mathfrak{M}\mathfrak{A}\pi$, where $\mathfrak{A}$ is a non zero ideal in the center $\mathbb{Q}[\sqrt{p}]$ of $\mathcal{H}$ and π a non zero two-sided ideal of $\mathfrak{N}$, because all two-sided $\mathfrak{M}$-ideals come from central ideals. Let π be a two-sided ideal of $\mathfrak{N}$ and $\mathfrak{M}' := End_{\mathfrak{M}\pi}(\mathfrak{M})$. The $\mathfrak{M}-\mathfrak{M}'$-lattices in $\mathcal{H}$ are the lattices $\mathfrak{M}\mathfrak{A}\pi$, where $\mathfrak{A}$ runs through the non zero ideals of $\mathbb{Q}[\sqrt{p}]$.

Let r be a rational prime that ramifies in $\mathcal{Q}$ and π_r the maximal two-sided ideal in $\mathfrak{N}$ containing r.

If r ramifies in $\mathbb{Q}[\sqrt{p}]$ then $rR = \mathfrak{A}_r{}^2$ where R is the maximal order of $\mathbb{Q}[\sqrt{p}]$ and $\mathfrak{A}_r \trianglelefteq R$. Completing $\mathfrak{M}$ and $\mathfrak{N}$ at $\mathfrak{A}_r$, one sees that $\mathfrak{M}\pi_r = \mathfrak{M}\mathfrak{A}_r$ Therefore $\mathfrak{M}\mathfrak{A}\pi\pi_r = \mathfrak{M}\mathfrak{A}\mathfrak{A}_r\pi$ is again an $\mathfrak{M}-\mathfrak{M}'$-lattice for every non zero ideal $\mathfrak{A}$ in $\mathbb{Q}[\sqrt{p}]$.

If r does not ramify in $\mathbb{Q}[\sqrt{p}]$ then r is inert (since $\mathcal{Q} \subseteq \mathcal{H}$) and therefore $\mathfrak{M}\pi\pi_r$ is not an $\mathfrak{M}-\mathfrak{M}'$-lattice. The proposition follows since $\mathfrak{M}\pi_r^2 = r\mathfrak{M}$. □

Convention. If C is a subalgebra of $M_n(\mathbb{Q})$ isomorphic to a number field K, C and K are identified and the matrices in C are referred to as to algebraic numbers. In particular an element $x \in C$ with $x^2 = p$ is denoted as $\sqrt{p}$ and ζ_k also means a primitive k-th root of unity in C.

The notation of [17, Proposition II.4] is used to describe finite matrix groups whose natural representation is close to a tensor product. In particular if $G \leq GL_n(\mathbb{Q})$ and H is a subgroup of the unit group of $End(G)$, then $G \circ H$ denotes the group generated by G and H. A 2 on top (sometimes followed by a natural number in brackets) indicates a certain extension of this group by a group of order 2.

2 The $SL_2(p)$-lattices of rank $2(p-1)$.

The aim of this section is to describe the faithful rational lattices of rank $2(p-1)$ of the group $SL_2(p)$, the group of the 2×2 matrices over the field with p elements of determinant 1, where p is a prime number.

The lattices of $SL_2(p)$ of rank $p-1$ (which belong to non faithful rational representations) have been described in [17, Chapter V b)]. They are cyclotomic lattices strongly related to Craig's lattices (cf. [5, p. 222]). The lattices of degree $2(p-1)$ turn out to have an interpretation as cyclotomic lattices over quaternion algebras.

To fix notation let $p > 3$ be a prime and $\zeta_{p+1} \in \mathbb{C}$ denote a primitive $(p+1)$-th root of unity. Let $A \in SL_2(p)$ be an element of order $p+1$. For $1 \leq i \leq \frac{p+1}{2}$ there is a unique character Θ_i of degree $p-1$ of $SL_2(p)$ with $\Theta_i(A) = -(\zeta_{p+1}^i + \zeta_{p+1}^{-i})$ (cf. [21]), which is the restriction of an irreducible character of $SL_2(p).2$. It is irreducible if $i \neq \frac{p+1}{2}$ and faithful if i is odd.

Immediately from the character table of $SL_2(p).2$ given in [21] (see also [7]) one gets the following

Lemma 2.1 *The faithful rational valued characters of degree $p-1$ of the group $SL_2(p)$ are the characters $\Theta_{\frac{p+1}{i}}$ for $i \in \{2,4,6\}$ dividing $p+1$ but not $\frac{p+1}{2}$.*

By [9, Theorem 6.1], all these faithful characters $\Theta_{\frac{p+1}{i}}$ have real Schur index 2. They lead to rational representations Δ_i of degree $n := 2(p-1)$ of $G := SL_2(p)$. A closer analysis of this Theorem yields the following

Lemma 2.2 *(i) If $p \equiv 1 \pmod 4$ then $End(\Delta_2(G)) \cong \mathcal{Q}_{\sqrt{p},\infty,\infty}$ is isomorphic to the quaternion algebra with center $\mathbb{Q}[\sqrt{p}]$ only ramified at the two infinite places.*

(ii) If $p \equiv 5 \pmod{12}$ then $End(\Delta_6(G)) \cong \mathcal{Q}_{\infty,3}$ is isomorphic to the quaternion algebra with center $\mathbb{Q}$ ramified at 3 and infinity.

(iii) If $p \equiv 3 \pmod 8$ then $End(\Delta_4(G)) \cong \mathcal{Q}_{\infty,2}$ is isomorphic to the quaternion algebra with center $\mathbb{Q}$ ramified at 2 and infinity.

The modular constituents of the Θ_i are already described in [17] and may be obtained from [4]. The only reference I found for the invariant bilinear form of (i) is [11, Theorem VI.1.1.] where the inverse is described:

Lemma 2.3 *Let r be a prime and $\hat{\Theta}_i$ denote the restriction of the character Θ_i to the r-regular classes, i.e. the conjugacy classes of elements of order not divisible by r, of $G = SL_2(p)$.*

(i) The irreducible $\mathbb{F}_pG$-modules are $\mathbb{F}_p[x,y]_s$, the spaces of homogenous polynomials of degree s ($0 \le s \le p-1$) with G-action defined by $x^{s-j}y^j \begin{pmatrix} a & b \\ c & d \end{pmatrix} := (ax+by)^{s-j}(cx+dy)^j$ for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, $0 \le j \le s$. $\mathbb{F}_p[x,y]_s$ is an absolutely irreducible $\mathbb{F}_pG$-module of dimension $s+1$. Its character will be denoted by β_{s+1}. Up to scalar multiples it has a unique G-invariant bilinear form $(,)$. The latter is defined by

$$(x^{s-j}y^j, x^{s-i}y^i) := (-1)^{s-j}\binom{s}{j}^{-1}\delta_{i,s-j} \quad (1 \le i,j \le s).$$

It is alternating if s is odd and symmetric if s is even.

(ii) If $r = p$ then $\hat{\Theta}_i = \beta_{i-1} + \beta_{p-i}$.

(iii) If $r \neq p$ let $i \in \{2,4,6\}$ divide $p+1$. The character $\hat{\Theta}_{\frac{p+1}{i}}$ is reducible if and only if $i = 2r$ or $i = 2$. In these cases $\hat{\Theta}_{\frac{p+1}{i}} = \hat{\Theta}_{\frac{p+1}{2}} = \hat{\Theta} + \hat{\Theta}'$ (where $\Theta_{\frac{p+1}{2}} =: \Theta + \Theta'$) decomposes as the sum of 2 characters of degree $\frac{p-1}{2}$.

Using this information one finds the following three Theorems:

Theorem 2.4 *Let $p \equiv 1 \pmod 4$, $G := SL_2(p)$, and $L \in \mathcal{L}(\Delta_2(G))$. Then the endomorphism ring $End_L(\Delta_2(G)) =: \mathfrak{M}$ is a maximal order of the endomorphism algebra $C := End(\Delta_2(G)) \cong \mathcal{Q}_{\sqrt{p},\infty,\infty}$. A system of representatives of isomorphism classes of $\mathfrak{M}\Delta_2(G)$-lattices is given by $L\mathfrak{A}$, where $0 \neq \mathfrak{A}$ runs through a set of representatives of the ideal classes of $\mathbb{Q}[\sqrt{p}] = Z(C)$. There is a unique ideal class, say represented by $\mathfrak{A}_0$, for which there exists a $F_0 \in \mathcal{F}_{>0}(G)$ such that $(L\mathfrak{A}_0, F_0)$ is unimodular.*

Denote this unimodular Euclidean lattice $(L\mathfrak{A}_0, F_0)$ by $L_{2(p-1),2}(\mathfrak{M})$.

Proof: By Lemma 2.3 the restrictions of the $\mathbb{C}$-constituents of the natural character of $\Delta_2(G)$ to the r-regular classes are irreducible Brauer characters of G for all primes r. Since the Sylow-p-subgroups of G are of order p, there is only one genus of $\Delta_2(G)$-lattices. Therefore $\mathfrak{M}$ is a maximal order in C. The $\mathfrak{M}\Delta_2(G)$-lattices correspond to two-sided ideals of $\mathfrak{M}$ hence are of the form $L\mathfrak{A}$, where $0 \neq \mathfrak{A}$ is an ideal in $\mathbb{Q}[\sqrt{p}]$.

Choose $F \in \mathcal{F}_{>0}(\Delta_2(G))$. By Lemma 1.1 (iii) the dual lattice $L^{\#,F}$ is again a $\mathfrak{M}\Delta_2(G)$-lattice. Hence $L^{\#,F} = L\mathfrak{B}$ for some ideal $\mathfrak{B}$ in $\mathbb{Q}[\sqrt{p}]$. Since by Lemma 1.1 (i) the form aF is symmetric for all $a \in \mathbb{Q}[\sqrt{p}]$, the dual lattice $(L\mathfrak{A})^{\#,F} = L\mathfrak{A}^{-1}\mathfrak{B}$ for all ideals $\mathfrak{A}$ of $\mathbb{Q}[\sqrt{p}]$. By [26, Theorem (10.4)(b)] the class number of $\mathbb{Q}[\sqrt{p}]$ is odd. So there is an ideal $\mathfrak{A}_0$ of $\mathbb{Q}[\sqrt{p}]$ and $b \in \mathbb{Q}[\sqrt{p}]$

such that $\mathfrak{B} = \mathfrak{A}_0^2(b)$. Since the fundamental unit of $\mathbb{Q}[\sqrt{p}]$ has norm -1 (cf. [26, Ex. (8.3)]) there is a totally positive generator b_0 of (b). Then $F_0 := b_0 F \in \mathcal{F}_{>0}(\Delta_2(G))$ and the lattice $(L\mathfrak{A}_0, F_0)$ is unimodular.

Let $(L\mathfrak{A}, xF)$ ($x \in \mathbb{Q}[\sqrt{p}]$ totally positive) be any other unimodular $\mathfrak{M}\Delta_2(G)$-lattice. Then $L\mathfrak{A} = (L\mathfrak{A})^{\#,xF} = L\mathfrak{B}\mathfrak{A}^{-1}x^{-1}$. Hence $\mathfrak{A}^{-2}\mathfrak{B}$ and therefore $(\mathfrak{A}^{-1}\mathfrak{A}_0)^2$ is principal. Again since the class number of $\mathbb{Q}[\sqrt{p}]$ is odd, this implies that the ideal class of $\mathfrak{A}$ is the one of $\mathfrak{A}_0$. □

Remark 2.5 (cf. [24]) *With the notation of Theorem 2.4 assume that $\mathfrak{M}$ contains a maximal order $\mathfrak{N}$ of the subalgebra $\mathcal{Q}_{\infty,p}$ of C. Then $L_{2(p-1),2}(\mathfrak{M})$ is invariant under an extension $SL_2(p).2$.*

Proof: By Proposition 1.2 $\mathfrak{M}$ is the unique maximal order of C containing $\mathfrak{N}$. The representation Δ_2 of G extends to a rational representation Δ_2 of both extensions $G.2$, with endomorphism algebra $End(\Delta_2(G.2)) \cong \mathcal{Q}_{\infty,p}$ (which may be calculated as the endomorphism algebra of the normalizer of a Sylow p-subgroup in $\Delta_2(G.2)$). Therefore the group $\Delta_2(G.2)$ fixes one of the $\mathfrak{N}\Delta_2(G)$-lattices, say L'. Since each $\Delta_2(G)$-lattice has a maximal order as its endomorphism ring, Proposition 1.2 implies that $End_{L'}(\Delta_2(G)) = \mathfrak{M}$. Hence L' is isomorphic to some $\mathfrak{M}\Delta_2(G)$-lattice $L\mathfrak{A}$. The $\mathfrak{N}\Delta_2(G.2)$-sublattices of L' are of the form $L'm$ or $L'm\pi$, where $m \in \mathbb{Z}$ and π denotes the maximal two-sided ideal of $\mathfrak{N}$ containing p. Since $L'\pi = L'\sqrt{p}$, all these lattices are isomorphic as $\mathfrak{M}\Delta_2(G)$-lattices. Now let $F \in \mathcal{F}_{>0}(\Delta_2(G.2))$ be primitive on L'. Then the dual lattice $L'^{\#,F}$ is either L' or $L'\sqrt{p}^{-1}$. In the first case $(L', F) = L_{2(p-1),2}(\mathfrak{M})$ is unimodular, in the second case $(L', \epsilon\sqrt{p}^{-1}F) = L_{2(p-1),2}(\mathfrak{M})$ is unimodular for a suitable fundamental unit $\epsilon \in \mathbb{Q}[\sqrt{p}]$. If $\Delta_2(G.2) = \langle \Delta_2(G), x\rangle$ then conjugation with x induces the Galois automorphism on $\mathbb{Q}[\sqrt{p}]$. Therefore the group $\langle \Delta_2(G), \epsilon x\rangle$ is a subgroup of $Aut(L', \epsilon\sqrt{p}^{-1}F)$. □

In the other two cases the group $\Delta_k(SL_2(p))$ ($k = 6$ resp. 4) is uniform and the endomorphism algebra has class number 1.

Theorem 2.6 *Let $p \equiv 5 \pmod{12}$ and $G := SL_2(p)$. Then the group $\Delta_6(G)$ is uniform. There is a $\Delta_6(G)$-invariant lattice L and $F \in \mathcal{F}_{>0}(G)$, such that $(L, F) =: L_{2(p-1),6}$ is primitive of determinant $p^{(p-5)/3}$. The endomorphism ring $End_L(\Delta_6(G))$ of L is a maximal order $\mathfrak{M}$ in the endomorphism algebra $C := End(\Delta_6(G)) \cong \mathcal{Q}_{\infty,3}$. If $p > 5$ then the two lattices L and $L^{\#,F}$ represent the isomorphism classes of $\mathfrak{M}\Delta_6(G)$-lattices in $\mathbb{Q}^n$. The primitive $\Delta_6(G)$-lattices having not a maximal order as endomorphism ring are unimodular. If $p = 5$ then $L_{8,6} = L_{8,6}^{\#}$ is unimodular, and hence isometric to E_8.*

Proof: The irreducible rational representation Δ_6 remains irreducible when considered over the reals (cf. Lemma 2.2). So the matrix group $\Delta_6(G)$ is

uniform. Let $L \in \mathcal{L}(\Delta_6(G))$ be a G-invariant lattice and F the positive definite $\Delta_6(G)$-invariant form, which is primitive on L.

Since $\mathbb{Q}_p C \cong M_2(\mathbb{Q}_p)$ the $\mathbb{Q}_p\Delta_6(G)$-module $\mathbb{Q}_p L = V_1 \oplus V_2$ is a sum of two isomorphic $\mathbb{Q}_p\Delta_6(G)$-modules each affording the character $\Theta_{\frac{p+1}{6}}$. Let $i = 1, 2$ and L_i be a $\mathbb{Z}_p\Delta_6(G)$-lattice in V_i. The Sylow p-subgroup of G is of order p, so the $\mathbb{Z}_p\Delta_6(G)$-sublattices of L_i in V_i are linearly ordered. By Lemma 2.3 the irreducible $\mathbb{F}_p\Delta_6(G)$-constituents of L_i/pL_i are absolutely irreducible of degree $\frac{p-5}{6}$ and $\frac{5p-1}{6}$. Replacing L by a maximal sublattice of p-power index if necessary, one may suppose that $\mathbb{Z}_p L$ is a direct sum of two isomorphic $\mathbb{Z}_p\Delta_6(G)$-lattices. Then $\mathbb{Z}_p\mathfrak{M} \cong M_2(\mathbb{Z}_p)$. The $\mathbb{Z}_p\mathfrak{M}\Delta_6(G)$-lattices in $\mathbb{Q}_p L$ are linearly ordered by inclusion and the $\mathbb{F}_p\mathfrak{M}\Delta_6(G)$ composition factors of L/pL are of dimension $2\frac{p-5}{6}$ and $2\frac{5p-1}{6}$. By Lemma 1.1 (iii) the dual lattice $L^{\#,F}$ is also an $\mathfrak{M}$-lattice. Therefore, the p-part of the determinant of L is one of $p^{2(p-5)/6}$ or $p^{2(5p-1)/6}$. Replacing (L, F) by $(L^{\#,F}, pF)$ if necessary, one achieves that the p-part of $\mathsf{det}(L, F)$ is $p^{(p-5)/3}$.

So it remains to consider the prime 3. As 3-Brauer character $\hat{\Theta}_{\frac{p+1}{6}} = \hat{\Theta} + \hat{\Theta}'$, but the character values of $\hat{\Theta}$ (and $\hat{\Theta}'$) generate $\mathbb{F}_3[\sqrt{p}] \cong \mathbb{F}_9$. So there is up to isomorphism only one $\mathbb{Z}_3\Delta_6(G)$-lattice in $\mathbb{Q}_3 L$. Therefore $\mathfrak{M}$ is a maximal order in C and L is invariant under the group $\Delta_6(G) \circ \tilde{S}_3 \leq GL_n(\mathbb{Q})$ generated by $\Delta_6(G)$ and the unit group $\tilde{S}_3$ of $\mathfrak{M}$. The 3-modular constituents of the natural character of $\Delta_6(G) \circ \tilde{S}_3$ are of degree $\frac{p-1}{2}$, where the lifts of the corresponding character values generate the biquadratic extension $\mathbb{Q}[\sqrt{p}, \zeta_4]$ of $\mathbb{Q}$. Since $-p$ is a square in $\mathbb{F}_3$, the $\mathbb{F}_3\Delta_6(G) \circ \tilde{S}_3$-module $L/3L$ has two non isomorphic composition factors L/L' and $L'/3L$. The corresponding 3-Brauer characters are complex, so L/L' is the dual module of $L'/3L$ and therefore 3 does not divide $\mathsf{det}(L, F)$.

Now let $p > 5$. The $\mathbb{F}_p G$-module $L^{\#,F}/L$ is isomorphic to $W_1 \oplus W_2$, where $W_i \cong \mathbb{F}_p[x, y]_s$ $(i = 1, 2)$ is the $\mathbb{F}_p G$-module of homogenous polynomials of degree $s := \frac{p-11}{6}$ of Lemma 2.3. Since s is odd the G-invariant bilinear form $(,)$ on W_i $(i = 1, 2)$ is alternating. Hence the symmetric bilinear form induced by F on $L^{\#,F}/L$ is $\langle w_1 + w_2, w_1' + w_2' \rangle = (\varphi(w_1), w_2') + (\varphi(w_1'), w_2)$ $(w_i \in W_i, i = 1, 2)$ where $\varphi : W_1 \to W_2$ is a G-isomorphism. The G-invariant subspaces of $L^{\#,F}/L$ are $M_i := \{w_1 + w_2 \in W_1 \oplus W_2 \mid \varphi(w_1) = iw_2\}$ $(i = 0, \ldots, p-1)$ and $M_p := W_1 \oplus \{0\}$. Hence $M_i^{\perp} = M_i$ $(0 \leq i \leq p)$ and the G-invariant overlattices containing L of index $p^{(p-5)/6}$ are unimodular. □

Theorem 2.7 *Let $p \equiv 3 \pmod 8$ and $G := SL_2(p)$. Then the group $\Delta_4(G)$ is uniform. There is a lattice $L \in \mathcal{L}(\Delta_4(G))$ and $F \in \mathcal{F}_{>0}(G)$, such that $(L, F) =: L_{2(p-1),4}$ is primitive of determinant $2^{p-1}p^{(p-3)/2}$. The endomorphism ring $End_{L_{2(p-1),4}}(\Delta_4(G))$ is a maximal order $\mathfrak{M}$ in $\mathcal{Q}_{\infty,2}$. The two lattices L*

and $L^{\#,F}$ represent the isomorphism classes of $\mathfrak{M}\Delta_4(G)$ lattices in $\mathbb{Q}^n$. The primitive $\Delta_4(G)$-lattices having not the maximal order as endomorphism ring have determinant 2^{p-1}.

Proof: The proof is analogous to the one of Theorem 2.6. But here one has to consider the prime 2 (instead of 3). Now the unit group of $\mathfrak{M}$ is $SL_2(3)$. Adjoining the lifts of the character values of the 2-modular constituents of the natural character of $\Delta_4(G) \circ SL_2(3)$ one obtains the character field $\mathbb{Q}[\sqrt{-p}, \zeta_3]$. Since $(-p)(-3) \equiv 1 \pmod 8$ the $\mathbb{F}_2\Delta_4(G) \circ SL_2(3)$-module $L/2L$ has 2 (different) constituents of degree $p-1$. But now, the corresponding 2-Brauer characters are real, which implies that the 2-part of $\mathsf{det}(L,F)$ is 2^{p-1}. □

Remark 2.8 *If $p = 11$ then $Aut(L_{20,4}) = SL_2(11) \overset{2(2)}{\circ} SL_2(3)$ acts transitively on the 12 $\Delta_4(SL_2(11))$-sublattices of index 11^8 in $L_{20,4}$. These sublattices are extremal 2-modular lattices with automorphism group $2.M_{12}.2$ (cf. [17, Lemma (IX.3)]).*

If $p = 19$ then $Aut(L_{36,4}) = SL_2(19) \overset{2(2)}{\circ} SL_2(3)$ has 2 orbits on the 20 $\Delta_4(SL_2(19))$-sublattices of index 19^{14} in $L_{36,4}$ of length 12 resp. 8. Both orbits consist of extremal 2-modular lattices (of minimum 6). The automorphism groups are $SL_2(19).2$ resp. $SL_2(19) \circ C_3$.

3 Cyclo-quaternionic lattices.

In this section an explicit construction for the lattices $L_{2(p-1),2}(\mathfrak{M})$ and $L_{2(p-1),6}$ for primes $p \equiv 1 \pmod 4$ is obtained. To find these lattices one has to construct a representation of a metacyclic group, which is certainly easier than constructing Δ_2 or Δ_6, but involves the problem of solving norm equations in abelian number fields if $p \equiv 1 \pmod 8$.

The fundamental observation is that for $k = 2$ and 6 the restriction of Δ_k to the Borel subgroup $B := {}^{\pm}C_p.C_{\frac{p-1}{2}} \leq SL_2(p)$ (the non split extension of a cyclic group ${}^{\pm}C_p$ of order $2p$ by the subgroup of index 2 in $Aut(C_p)$) remains rationally irreducible. Note that $\frac{p-1}{2}$ is even because $p \equiv 1 \pmod 4$ in these two cases.

Since B has only one rational irreducible faithful representation Δ the restrictions of the two representations Δ_2 and Δ_6 to B coincide for $p \equiv 5 \pmod{12}$. The endomorphism algebra $C := End(\Delta(B))$ is $\mathcal{Q}_{\sqrt{p},\infty,\infty}$. The center of C will be identified with $\mathbb{Q}[\sqrt{p}]$.

Lemma 3.1 *Let $\Delta(B) = \langle z, a\rangle \leq GL_{2(p-1)}(\mathbb{Q})$, where $\langle z\rangle \trianglelefteq \Delta(B)$ is the normal p-subgroup of $\Delta(B)$, $a^{(p-1)/2} = -1$, and conjugation with a induces a Galois automorphism of order $\frac{p-1}{2}$ of $\mathbb{Q}[z] \cong \mathbb{Q}[\zeta_p]$.*

Then $\wp := ((1-z)a)^{(p-1)/4} \in N_{GL_{2(p-1)}(\mathbb{Q})}(\Delta(B))$ *normalizes* $\Delta(B)$.

Proof: Straightforward:
$\wp = (1-z)(a(1-z)a^{-1})(a^2(1-z)a^{-2})\dots(a^{(p-1)/4-1}(1-z)a^{1-(p-1)/4})a^{(p-1)/4}$, where the first $\frac{p-1}{4}$ factors pairwise commute. Since these factors also commute with z, one has $z^\wp = z^{-1}$. Moreover $a^\wp = (1-z^{-1})(1-z)^{-1}a = -z^{-1}a$. □

Note that $-\wp^2$ is the norm of $\mathbb{Q}[z]/\mathbb{Q}[\sqrt{p}]$ of $(1-z)$ and hence a totally positive generator of the ideal $(\sqrt{p})$ of $\mathbb{Q}[\sqrt{p}]$.

Proposition 3.2 *Let* $\mathfrak{M}$ *be a maximal order of* C, $F \in \mathcal{F}_{>0}(\Delta(B))$, *and* $L \in \mathcal{L}(\Delta(B))$ *with* $End_L(\Delta(B)) = \mathfrak{M}$. *Let* S *be a system of non zero representatives of the ideal classes of* $Z(C) = \mathbb{Q}[\sqrt{p}]$.

(i) The $\mathfrak{M}\Delta(B)$ *sublattices of p-power index in* L *are* $L =: L^{(0)} \supset L^{(1)} \supset L^{(2)} \supset \dots \supset L^{(\frac{p-1}{2})} = \sqrt{p}L$ *with* $|L^{(i)}/L^{(i+1)}| = p^2$ *for all* $0 \le i < \frac{p-1}{2}$. *The lattices* $L^{(0)}\mathfrak{A}, \dots, L^{(\frac{p-3}{2})}\mathfrak{A}$ *with* $\mathfrak{A} \in S$ *form a system of representatives of isomorphism classes of* $\mathfrak{M}\Delta(B)$*-lattices in* $\mathbb{Q}^{2(p-1)}$.

(ii) Let $\wp$ *be as in Lemma 3.1. If* $i \in \{0, \dots, \frac{p-5}{4}\}$ *then* $L^{(i+\frac{p-1}{4})}\mathfrak{A} = L^{(i)}\wp\mathfrak{A}$ *and* $(L^{(i)}\wp\mathfrak{A}, F)$ *is isometric to* $(L^{(i)}\mathfrak{A}, -\wp^2 F)$.

(iii) There is a unique $i_0 \in \{0, \dots, \frac{p-5}{4}\}$ *for which the lattices* $L^{(i_0)}\mathfrak{A}$, $\mathfrak{A} \in S$, *are invariant under* $\Delta_2(SL_2(p)) \le Aut(L^{(i_0)}\mathfrak{A}, F)$.

Replacing L *by* $L^{(i_0)}\mathfrak{A}_0$ *for a suitable ideal* $\mathfrak{A}_0$ *of* $\mathbb{Q}[\sqrt{p}]$ *and choosing an appropriate* $F \in \mathcal{F}_{>0}(\Delta(B))$ *(as in Theorem 2.4) one achieves that* $(L, F) = L_{2(p-1),2}(\mathfrak{M})$ *is unimodular.*

(iv) Assume that $\mathfrak{M}$ *contains a maximal order* $\mathfrak{M}_{\infty,3}$ *of* $\mathcal{Q}_{\infty,3}$. *If* $(L, F) = L_{2(p-1),2}(\mathfrak{M})$ *is the unimodular lattice of (iii), then* $(L^{(\frac{p-5}{12})}, F) = L_{2(p-1),6}$ *is invariant under* $\Delta_6(SL_2(p)) \le Aut(L^{(\frac{p-5}{12})}, F)$.

Proof: (i) Let $\langle z \rangle \trianglelefteq \Delta(B)$ be the normal p-subgroup of $\Delta(B)$. The order $\mathfrak{M}\langle z \rangle$ is isomorphic to $M_2(\mathbb{Z}[\zeta_p])$. So the $\mathfrak{M}\Delta(B)$ sublattices of L correspond to the ideals of $\mathbb{Z}[\zeta_p]$ which are stable under the Galois group $Gal(\mathbb{Q}[\zeta_p]/\mathbb{Q}[\sqrt{p}])$. Hence a system of representatives of isomorphism classes of $\mathfrak{M}\Delta(B)$-lattices is given by $L^{(i)}\mathfrak{A} = L(1-z)^i\mathfrak{A}$ where $\mathfrak{A} \in S$ and $0 \le i \le \frac{p-3}{2}$.
(ii) By Lemma 3.1 $\wp \in N_{GL_{2(p-1)}(\mathbb{Q})}(\Delta(B))$ is an element of determinant $p^{(p-1)/2}$ normalizing $\Delta(B)$. Since $\wp$ lies in the enveloping algebra of $\Delta(B)$, it commutes with C. Therefore the lattice $L^{(i)}\wp\mathfrak{A}$ is a $\mathfrak{M}\Delta(B)$-sublattice of index $p^{(p-1)/2}$ of $L^{(i)}\mathfrak{A}$ and hence equals $L^{(i+\frac{p-1}{4})}\mathfrak{A}$ by (i). Clearly $(L^{(i)}\wp\mathfrak{A}, F)$ is isometric to $(L^{(i)}\mathfrak{A}, \wp F \wp^{tr})$. Since $\wp$ normalizes $\Delta(B)$, the form $\wp F \wp^{tr}$ lies in $\mathcal{F}_{>0}(\Delta(B))$.

With Lemma 1.1 (i) one gets that $\wp F \wp^{tr} = -x\wp^2 F$ for some totally positive unit $x \in \mathbb{Q}[\sqrt{p}]$. Since the fundamental unit of $\mathbb{Q}[\sqrt{p}]$ has norm -1 the unit $x = y^2$ is a square and y yields an isometry between $(L^{(i)}\mathfrak{A}, -x\wp^2 F)$ and $(L^{(i)}\mathfrak{A}, -\wp^2 F)$.
(iii) The group $\Delta_2(SL_2(p))$ contains a group $\Delta(B)$. Since C is also the endomorphism algebra of $\Delta_2(SL_2(p))$ one has $\mathcal{F}(\Delta_2(SL_2(p))) = \mathcal{F}(\Delta(B))$ and there is a $0 \leq i_0 \leq \frac{p-3}{2}$ such that $\mathfrak{M}\Delta_2(SL_2(p))$ fixes the lattices $L^{(i_0)}\mathfrak{A}$ ($\mathfrak{A} \in S$). By Theorem 2.4 there is an ideal $\mathfrak{A}_0$ of $\mathbb{Q}[\sqrt{p}]$ such that $(L^{(i_0)}\mathfrak{A}_0, bF)$ is unimodular for some totally positive $b \in \mathbb{Q}[\sqrt{p}]$. If $i_0 > \frac{p-5}{4}$ one applies the isometry $\wp^{-1}$ of (ii) and replaces F by $-\wp^2 F$ to achieve $0 \leq i_0 \leq \frac{p-5}{4}$. The uniqueness of such an i_0 follows because the determinant $\mathsf{det}(L^{(i_0+i)}\mathfrak{A}_0, bF) = p^{4i}$ ($1 \leq i \leq \frac{p-5}{4}$) is > 1 and not divisible by $p^{p-1} = \mathsf{det}(\wp^2)$.
(iv) Since $\mathcal{Q}_{\infty,3} \leq \mathcal{Q}_{\sqrt{p},\infty,\infty}$, one has $p \equiv 5 \pmod{12}$ and 3 is inert in $\mathbb{Q}[\sqrt{p}]$. The lattices $L^{(i)}\mathfrak{A}$ together with $L^{(i)}\pi\mathfrak{A}$ ($0 \leq i \leq \frac{p-3}{2}$, $\mathfrak{A} \in S$), where π is a generator of the maximal two-sided ideal of $\mathfrak{M}_{\infty,3}$ containing 3, form a system of representatives of isomorphism classes of $\mathfrak{M}_{\infty,3}\Delta(B)$-lattices. Among these there is a lattice L', on which $\Delta_6(SL_2(p))$ acts. But then $\Delta_6(SL_2(p))$ also fixes the lattice $L'\pi$. With (ii) the lattice $(L^{(\frac{p-5}{12})}, F)$ is up to isometry the unique $\mathfrak{M}\Delta(B)$-lattice of determinant $p^{\frac{p-5}{6}}$ and (iv) follows from Theorem 2.6. □

The following tables display some invariants of the cyclo-quaternionic lattices for $p = 5$, 13, 17, and 29. Here the class number of $\mathbb{Q}[\sqrt{p}]$ is one. The first line contains the name of the lattice, where it is assumed that $(L^{(0)}, F) = L_{2(p-1),2}(\mathfrak{M})$ is unimodular. The quadratic form F is omitted and $L_{2(p-1),2}(\mathfrak{M})$ is shortly denoted by $L_{2(p-1),2}$, if $\mathfrak{M}$ is unique up to conjugacy. The second row contains the determinant. The last three rows contain the minimum, the number of minimal vectors, resp. the rounded value of the Hermite parameter of the lattice, if these data could be computed.

$p=5$	$L_{8,2}$	$L^{(1)}_{8,2}$	$p=13$	$L_{24,2}$	$L^{(1)}_{24,2}$	$L^{(2)}_{24,2}$	$L^{(3)}_{24,2}$	$L^{(4)}_{24,2}$	$L^{(5)}_{24,2}$
$\mathsf{det}(L)$	1	5^4		1	13^4	13^8	13^{12}	13^{16}	13^{20}
$\mathsf{min}(L)$	2	4		4	4	6	12	14	24
$\lvert L_{min}\rvert$	240	120		196560	936	1248	13104	312	1248
$\gamma(L)$	2	1.79		4	2.61	2.55	3.33	2.53	2.83

$p=17$	$L_{32,2}$	$L^{(1)}_{32,2}$	$L^{(2)}_{32,2}$	$L^{(3)}_{32,2}$	$L^{(4)}_{32,2}$	$L^{(5)}_{32,2}$	$L^{(6)}_{32,2}$	$L^{(7)}_{32,2}$
$\mathsf{det}(L)$	1	17^4	17^8	17^{12}	17^{16}	17^{20}	17^{24}	17^{28}
$\mathsf{min}(L)$	4	6	8	10	12	20	30	44
$\lvert L_{min}\rvert$	146880	233376	63648	4896	1632	3264	4896	4896
$\gamma(L)$	4	4.21	3.94	3.46	2.91	3.40	3.58	3.69

There are two non conjugate maximal orders $\mathfrak{M}$ and $\tilde{\mathfrak{M}}$ in the quaternion algebra $\mathcal{Q}_{\sqrt{29},\infty,\infty}$. They correspond to the two different constructions $\mathcal{Q}_{\sqrt{29},\infty,\infty} = \mathbb{Q}[\sqrt{29}] \otimes \mathcal{Q}_{\infty,2} = \mathbb{Q}[\sqrt{29}] \otimes \mathcal{Q}_{\infty,3}$ and can be distinguished by the property that $\mathfrak{M}$ contains a maximal order of $\mathcal{Q}_{\infty,2}$ and $\tilde{\mathfrak{M}}$ a maximal order of $\mathcal{Q}_{\infty,3}$. One obtains the following numerical results:

$p=29$	$L_{56,2}(\mathfrak{M})$	$L^{(1)}_{56,2}(\mathfrak{M})$	$L^{(2)}_{56,2}(\mathfrak{M})$	$L^{(3)}_{56,2}(\mathfrak{M})$	$L^{(4)}_{56,2}(\mathfrak{M})$	$L^{(5)}_{56,2}(\mathfrak{M})$	$L^{(6)}_{56,2}(\mathfrak{M})$
$\mathsf{det}(L)$	1	29^4	29^8	29^{12}	29^{16}	29^{20}	29^{24}
$\mathsf{min}(L)$	6	6	8	10	12	16	20
$\lvert L_{min}\rvert$	15590400	9744	58464	146160	204624	53592	9744
$\gamma(L)$	6	4.72	4.95	4.86	4.59	4.81	4.72
$p=29$	$L_{56,2}(\tilde{\mathfrak{M}})$	$L^{(1)}_{56,2}(\tilde{\mathfrak{M}})$	$L^{(2)}_{56,2}(\tilde{\mathfrak{M}})$	$L^{(3)}_{56,2}(\tilde{\mathfrak{M}})$	$L^{(4)}_{56,2}(\tilde{\mathfrak{M}})$	$L^{(5)}_{56,2}(\tilde{\mathfrak{M}})$	$L^{(6)}_{56,2}(\tilde{\mathfrak{M}})$
$\mathsf{det}(L)$	1	29^4	29^8	29^{12}	29^{16}	29^{20}	29^{24}
$\mathsf{min}(L)$	6	6	10	≤ 12	≤ 14	≤ 16	≤ 20
$\gamma(L)$	6	4.72	6.18	≤ 5.83	≤ 5.35	≤ 4.81	≤ 4.72

$p=29$	$L^{(7)}_{56,2}(\mathfrak{M})$	$L^{(8)}_{56,2}(\mathfrak{M})$	$L^{(9)}_{56,2}(\mathfrak{M})$	$L^{(10)}_{56,2}(\mathfrak{M})$	$L^{(11)}_{56,2}(\mathfrak{M})$	$L^{(12)}_{56,2}(\mathfrak{M})$	$L^{(13)}_{56,2}(\mathfrak{M})$
$\mathsf{det}(L)$	29^{28}	29^{32}	29^{36}	29^{40}	29^{44}	29^{48}	29^{52}
$\mathsf{min}(L)$	28	28	28	28	58	88	116
$\lvert L_{min}\rvert$	107880	696	696	696	9744	19488	24360
$\gamma(L)$	5.20	4.09	3.21	2.53	4.12	4.91	5.09
$p=29$	$L^{(7)}_{56,2}(\tilde{\mathfrak{M}})$	$L^{(8)}_{56,2}(\tilde{\mathfrak{M}})$	$L^{(9)}_{56,2}(\tilde{\mathfrak{M}})$	$L^{(10)}_{56,2}(\tilde{\mathfrak{M}})$	$L^{(11)}_{56,2}(\tilde{\mathfrak{M}})$	$L^{(12)}_{56,2}(\tilde{\mathfrak{M}})$	$L^{(13)}_{56,2}(\tilde{\mathfrak{M}})$
$\mathsf{det}(L)$	29^{28}	29^{32}	29^{36}	29^{40}	29^{44}	29^{48}	29^{52}
$\mathsf{min}(L)$	20	32	≤ 42	≤ 56	≤ 68	≤ 98	≤ 108
$\lvert L_{min}\rvert$	4872	9744					
$\gamma(L)$	3.71	4.67	≤ 4.82	≤ 5.05	≤ 4.82	≤ 5.47	≤ 4.74

With programs, developed by H. Napias [12], which allow to perform an LLL-reduction over Euclidean domains, one obtains LLL-reduced bases for the lattices $L^{(i)}_{56,2}(\mathfrak{M})$ (resp. $L^{(i)}_{56,2}(\tilde{\mathfrak{M}})$) viewed as lattices over the maximal order in $\mathcal{Q}_{\infty,2}$ (resp. $\mathcal{Q}_{\infty,3}$) which is contained in $\mathfrak{M}$ (resp. $\tilde{\mathfrak{M}}$). Whereas for the first lattices it is possible to calculate the minimal vectors, PARI does not produce results for the lattices $L^{(i)}_{56,2}(\tilde{\mathfrak{M}})$ $(1 \leq i \neq 7,8)$ after 1 week of calculations. The upper bounds for the minima of these lattices are obtained from an LLL-reduced basis and the minimum of $L^{(2)}_{56,2}(\tilde{\mathfrak{M}})$ will be proved in the next section.

Remark 3.3 *The lattices $L^{(i)}_{2(p-1),2}(\mathfrak{M})$ have a purely algebraic interpretation as ideals of the maximal order $\mathfrak{O} := \mathbb{Z}[\zeta_p + \zeta_p^{-1}] \otimes_{\mathbb{Z}[\frac{1+\sqrt{p}}{2}]} \mathfrak{M}$ of the quaternion algebra $\mathbb{Q}\mathfrak{O}$ with center $\mathbb{Q}[\zeta_p + \zeta_p^{-1}]$ ramified only at the $\frac{p-1}{2}$ infinite places.*

There are two remarkable lattices in these tables, $L_{32,2}^{(1)} = L_{32,6}$ and $L_{56,2}^{(2)}(\tilde{\mathfrak{M}}) = L_{56,6}$, which are denser than the corresponding extremal unimodular lattices. These lattices also have an interpretation as Mordell-Weil lattices as shown in the next section.

4 Connection with Mordell-Weil lattices.

In [23], Shioda investigates the Mordell-Weil lattice of the elliptic curve

$$E: \ y^2 = x^3 + 1 + t^{p+1}$$

over the rational function field $k(t)$, where k is any field of characteristic p containing $\mathbb{F}_{p^2}$ and p is a prime $\equiv -1 \pmod 6$. He shows that with respect to the canonical height h the group of $k(t)$-rational points $E(k(t))$ is a positive definite even lattice of rank $2p-2$, determinant $p^{(p-5)/3}$ and minimal norm $\frac{p+1}{3}$. (These lattices have been independently discovered by N.D. Elkies.)

Let $K := \mathbb{F}_{p^2}(t)$. Since the Frobenius automorphism $a \mapsto a^p$ generates the Galois group $Gal(\mathbb{F}_{p^2}/\mathbb{F}_p)$ the unitary group $U_2(\mathbb{F}_{p^2})$, isomorphic to an extension of the central product of a cyclic group of order $p+1$ and $SL_2(p)$ by a group of order 2, acts on the K-rational points of the Fermat curve $X_{p+1}: \ x_1^{p+1} + x_2^{p+1} = t^{p+1} + 1$. The mapping $(x_1, x_2) \mapsto (-x_1^{(p+1)/3}, x_2^{(p+1)/2})$ defines a dominant rational mapping from X_{p+1} to E. So one is tempted to induce the action of $U_2(\mathbb{F}_{p^2})$ on $E(K)$. But this induced action on $E(K)$ is not well defined. However one gets:

Theorem 4.1 *If $p \equiv -1 \pmod 6$ then the group $G := U_2(\mathbb{F}_{p^2})$ acts on the lattice $(E(K), h)$ via isometries. The kernel of this action is the subgroup of order $\frac{p+1}{6}$ of the center $Z(G) \cong C_{p+1}$.*

Proof: The strategy of the proof is to define an action of G on a subset S of vectors of norm $\frac{p+1}{3}$ in $E(K)$. The kernel of this action is the subgroup of index 6 in the center $Z(G)$. The image H acts as isometries (with respect to h) on this subset S of the free abelian group $E(K)$, hence linear on the $\mathbb{Q}$-vector space spanned by S. Since H has no faithful rational representation of degree $< 2(p-1)$, the subset S generates a full H-invariant sublattice L of $E(K)$. The most difficult part of the proof is the identification of L with $E(K)$. For this purpose a sublattice of rank 4 of L on which a certain element of order $p+1$ in G acts as 6th root of unity is compared with the corresponding sublattices of the other G-lattices of dimension $2(p-1)$ using an explicit description of the group ring. Elkies pointed out a much easier proof of Theorem 4.1 which is sketched in Remark 4.8.

The subset $S \subseteq E(K)$. With [23, Proposition 5.3] one finds:
The elements $(x_1, x_2) \in X_{p+1}(\mathbb{F}_{p^2}[t])$ such that x_1 and x_2 are of degree 1 are of the form $x_1 = at + b$, $x_2 = ct + d$, where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ is an element of the unitary group $G = U_2(\mathbb{F}_{p^2})$.

Define S to be the set of images of these points:

$$S := \{(x, y) = (-(at+b)^{(p+1)/3}, (ct+d)^{(p+1)/2}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in U_2(\mathbb{F}_{p^2})\}$$

The action of G on S. Let ζ denote a primitive $(p+1)$-th root of unity in $\mathbb{F}_{p^2}$. The preimages of $(x, y) = (-(at+b)^{(p+1)/3}, (ct+d)^{(p+1)/2}) \in S$ are of the form $(\zeta^{3\alpha}(at+b), \zeta^{2\beta}(ct+d))$. They form a full right coset of the subgroup $U := \langle \begin{pmatrix} \zeta^3 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & \zeta^2 \end{pmatrix} \rangle \cong C_{\frac{p+1}{3}} \times C_{\frac{p+1}{2}} \leq G$. Identifying S with the set of right cosets $U\backslash G$, one gets an action of G on S induced by right multiplication in G. The kernel is the largest normal subgroup of G contained in U, $core(U) = U \cap Z(G) \cong C_{\frac{p+1}{6}}$.

That this action of G on S induces isometries of the lattice (L, h), may be seen by a direct calculation of the scalar products: Let $P, Q \in S$. Viewing the points on $E(K)$ as elements $(P), (Q)$ of the Néron-Severi group of the corresponding elliptic surface and taking into account, that this surface has no reducible fibers and that P and Q do not intersect with the zero divisor, one calculates $\langle P, Q \rangle = \frac{p+1}{6} - ((P)(Q))$ (cf. [22]), where $((P)(Q))$ is the intersection number of the two divisors (P) and (Q) and $\langle ., . \rangle$ is the bilinear form whose associated quadratic form $\langle P, P \rangle = h(P)$ is the canonical height.

Let $P := (-(at+b)^{(p+1)/3}, (ct+d)^{(p+1)/2})$ and $Q := (-(\alpha t+\beta)^{(p+1)/3}, (\gamma t + \delta)^{(p+1)/2})$ be in S.

The value $t \in \mathbb{P}^1(\mathbb{F}_{p^2}) = \mathbb{F}_{p^2} \cup \{\infty\}$ gives an intersection point of (P) and (Q), if $(at+b) = \zeta^{3r}(\alpha t + \beta)$ and $(ct+d) = \zeta^{2s}(\gamma t + \delta)$ for some r, s.

If

$$\text{(gen)} \quad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \neq \begin{pmatrix} \zeta^i & 0 \\ 0 & \zeta^j \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ for all } 1 \leq i, j \leq p+1$$

then $((P)(Q))$ is the number of solutions $0 \leq r < \frac{p+1}{3}$, $0 \leq s < \frac{p+1}{2}$ of

$$(\star) \quad (\alpha\delta - \beta\gamma)\zeta^{3r+2s} + (\beta c - \alpha d)\zeta^{3r} + (b\gamma - a\delta)\zeta^{2s} + ad - bc = 0.$$

Namely then each solution of $(\star)$ gives an intersection at $t = t(r, s) = \frac{\beta\zeta^{3r} - b}{a - \alpha\zeta^{3r}} = \frac{\delta\zeta^{2s} - d}{c - \gamma\zeta^{2s}} \in \mathbb{F}_{p^2} \cup \{\infty\}$. If equality holds in the condition (gen) for some (i, j) and $P \neq Q$, then $P \oplus [(-1)^j]Q \in S$, hence $\langle P, Q \rangle = (-1)^{j+1}\frac{p+1}{6}$.

Clearly the condition (gen) is invariant under right multiplication with elements of G. If one replaces P by Pg and Q by Qg, the equation $(\star)$ for

$((Pg)(Qg))$ is multiplied by the determinant of $g \in G$. Therefore G acts as isometries, hence linear, on $L = \langle S \rangle$.

We now want to show that L equals $E(K)$. To this aim let $A \in SL_2(p) = SU_2(\mathbb{F}_{p^2})$ an element of order $p+1$, $A := \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$. Let

$$X := \langle (-t^{(p+1)/3}, 1), (-(\zeta t)^{(p+1)/3}, 1), (-1, t^{(p+1)/2}), (-\zeta^{(p+1)/3}, t^{(p+1)/2}) \rangle \leq L.$$

Then (X, h) is isometric to ${}^{(\frac{p+1}{6})}A_2^2$ a rescaling of an orthogonal sum of two copies of the hexagonal lattice. In particular $\mathsf{min}(X,h) = \frac{p+1}{3}$ and $\mathsf{det}(X,h) = (\frac{p+1}{6})^4 \cdot 3^2$. The eigenvalues of the matrix describing the action of A on X are primitive 6th roots of unity. The normalizer in $SL_2(p)$ of $\langle A \rangle$ is $N := \langle A, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \rangle$, a quaternion group of order $2(p+1)$. It also fixes the lattice X.

To identify L, the sublattices T of $SL_2(p)$-invariant lattices corresponding to the suitable homogenous component of N are investigated. Let $\psi^{(\beta)}$ denote the complex irreducible character of $\langle A \rangle$ defined by $\psi^{(\beta)}(A) := \zeta_{p+1}^{\beta}$ $(0 \leq \beta \leq p)$ where $\zeta_{p+1} \in \mathbb{C}$ is a primitive $(p+1)$-th root of unity and let ψ_β be the irreducible character of N whose restriction to $\langle A \rangle$ is $\psi^{(\beta)} + \psi^{(-\beta)}$ $(0 < \beta < \frac{p+1}{2})$ and ψ, ψ' be the two different extensions of $\psi^{(\frac{p+1}{2})}$ to N.

Lemma 4.2 *With the notation above let* $p \equiv -1 \pmod 6$, $N = \langle A \rangle.C_2 \cong C_{p+1}.C_2$ *be the quaternion group of order* $2(p+1)$, q *a prime, and* q^a *the maximal* q*-power dividing* $p+1$. *If* $q = 3$ *and* $p \equiv 1 \pmod 4$ *let* $K := \mathbb{Q}_3[\sqrt{p}]$ *be the unramified extension of degree 2 of* $\mathbb{Q}_3$, $K := \mathbb{Q}_q$ *in all the other cases, and* R *the maximal order in* K. *Let* $\alpha := \frac{p+1}{6}$, e_α *the centrally primitive idempotent in* KN *belonging to* ψ_α, *and* Λ *the block of* RN *containing a non zero multiple of* e_α. *Assume* $a \geq 1$.

(i) *If* $q \geq 5$, *then* $e_\alpha\Lambda/(e_\alpha\Lambda \cap \Lambda) \cong (R/q^aR)^4$ *as* R*-modules.*

(ii) *Let* $q = 3$ *and* e *resp.* e' *be the centrally primitive idempotents of* KN *belonging to* ψ *resp .* ψ'. *Let* $\Lambda_a := (1-e-e')\Lambda$. *Then* $e_\alpha\Lambda_a/(e_\alpha\Lambda_a \cap \Lambda_a) \cong (R/3^{a-1}R)^4$ *and* $e_\alpha\Lambda/(e_\alpha\Lambda \cap \Lambda) \cong (R/3^aR)^2 \oplus (R/3^{a-1}R)^2$ *as* R*-modules.*

(iii) *Let* $q = 2$ *and* $p \equiv 3 \pmod 4$. *View* ψ_α *as a character of* $\bar{N} := N/Z(N) \cong D_{p+1}$. *Let* $\bar{e}_\alpha$ *be the corresponding idempotent and* $\bar{\Lambda}$ *be the corresponding block of* $\mathbb{Z}_2\bar{N}$. *Then* $\bar{e}_\alpha\bar{\Lambda}/(\bar{e}_\alpha\bar{\Lambda} \cap \bar{\Lambda}) \cong (\mathbb{Z}/2^{a-1}\mathbb{Z})^4$.

Proof: In all cases the defect group of Λ is $C_{q^a} \leq \langle A \rangle$ and R/qR is a minimal splitting field for $\Lambda/q\Lambda$.
(i) From [16, Theorem (VIII.5)] one finds that Λ is of the form

$$\Lambda = \{(x,y) \in (1-e_\alpha)\Lambda \oplus e_\alpha\Lambda \mid \nu(x) = \mu(y)\}$$

where μ and ν are epimorphisms of the resp. orders onto $M_2(R/q^aR)$. Hence the amalgamation module of $e_\alpha\Lambda$ and $(1-e_\alpha)\Lambda$ is $e_\alpha\Lambda/(e_\alpha\Lambda\cap\Lambda)\cong(e_\alpha\Lambda+(1-e_\alpha)\Lambda)/\Lambda\cong(R/q^aR)^4$.
(ii) Now $q=3$ and the character ψ_α belongs to the exceptional vertex of the Brauer tree of Λ.

For $s=1,\ldots,a$ let $e_{\alpha/3^{s-1}}$ be the centrally primitive idempotent of KN belonging to the character

$$\Psi_{\alpha/3^{s-1}}:=\sum_{x=1,3\not| x}^{3^s}\psi_{x\alpha/3^{s-1}}$$

and $\Lambda_s:=\sum_{i=1}^s e_{\alpha/3^{i-1}}\Lambda$. According to [16, Theorem (VIII.5) (i)]

$$\Lambda_s=\{(x,y)\in\Lambda_{s-1}\oplus e_{\alpha/3^{s-1}}\Lambda\mid\nu_s(x)=\mu_s(y)\},$$

where $\mu_s: e_{\alpha/3^{s-1}}\Lambda\to e_{\alpha/3^{s-1}}\Lambda/Jac(e_{\alpha/3^{s-1}}\Lambda)^{3^{s-1}-1}$ and $\nu_s:\Lambda_{s-1}\to\Lambda_{s-1}/3\Lambda_{s-1}\cong e_{\alpha/3^{s-1}}\Lambda/Jac(e_{\alpha/3^{s-1}}\Lambda)^{3^{s-1}-1}$ are the canonical epimorphisms. We claim that $\Lambda_1\cap\Lambda_s=3^{s-1}\Lambda_1$. This is trivial for $s=1$. Assume that it is true for some $a>s\geq 1$. Let $x=x_1+\ldots+x_{s+1}\in\Lambda_1\cap\Lambda_{s+1}$, where $x_i\in e_{\alpha/3^{i-1}}\Lambda$ $(1\leq i\leq s+1)$. Since $x\in\Lambda_1$ and Λ_{s+1} is a subdirect sum of the $e_{\alpha/3^{i-1}}\Lambda$ $(1\leq i\leq s+1)$, this implies $x_2=\ldots=x_{s+1}=0$. Hence $x_1\in\Lambda_1\cap\Lambda_s$ with $\nu_{s+1}(x_1)=x_1+3\Lambda_s=0$. Therefore $x=x_1=3y$ with $y\in\Lambda_s$. Now $\Lambda_s\cap(\mathbb{Q}_3\Lambda_1)\subseteq\Lambda_1$, again because Λ_s is a subdirect sum. Hence $y\in\Lambda_s\cap\Lambda_1=3^{s-1}\Lambda_1$ and $x\in 3^s\Lambda_1$.

Since $\Lambda_1=e_\alpha\Lambda_a$, this implies $e_\alpha\Lambda_a/(e_\alpha\Lambda_a\cap\Lambda_a)\cong\Lambda_1/3^{a-1}\Lambda_1\cong(R/3^{a-1}R)^4$.

As in (i) the block Λ of RN is of the form $\Lambda=\{(x,y)\in\Lambda_a\oplus(e+e')\Lambda\mid\nu(x)=\mu(y)\}$. Here μ and ν are homomorphisms of the resp. orders onto $(R/3^aR)\oplus(R/3^aR)$. Hence the total amalgamation module $e_\alpha\Lambda/(e_\alpha\Lambda\cap\Lambda)$ is isomorphic to $(R/3^aR)^2\oplus(R/3^{a-1}R)^2$.
(iii) Since the degree of the irreducible Brauer character belonging to $\bar\Lambda$ is even, a defect group of $\bar\Lambda$ is isomorphic to $C_{2^{a-1}}\leq\bar N$. The idempotent $\bar e_\alpha$ belongs to the exceptional vertex of the Brauer tree of $\bar\Lambda$.

Let $\bar e_{2\alpha}$ be the centrally primitive idempotent of $K\bar N$ belonging to the character $\psi_{2\alpha}$ (of $\bar N$) and $\bar\Lambda_{a-1}:=(1-\bar e_{2\alpha})\bar\Lambda$. As in (ii) $\bar e_\alpha\bar\Lambda_{a-1}/(\bar e_\alpha\bar\Lambda_{a-1}\cap\bar\Lambda_{a-1})\cong(\mathbb{Z}/2^{a-2}\mathbb{Z})^4$. As in (i) $\bar\Lambda=\{(x,y)\in(1-\bar e_{2\alpha})\bar\Lambda\oplus\bar e_{2\alpha}\bar\Lambda\mid\nu(x)=\mu(y)\}$ where μ and ν are epimorphisms of the resp. orders onto $(\mathbb{Z}/2^{a-1}\mathbb{Z})^4$ from which one gets (iii). □

Lemma 4.3 *Let $p\equiv 5 \pmod{12}$ and (M,F) be a primitive lattice of dimension $2(p-1)$ with $(SL_2(p)\circ\tilde S_3).2\leq Aut((M,F))$. With the notation above let $T:=(\epsilon_\alpha+\epsilon_{-\alpha})M\cap M\leq M$ where $\alpha:=\frac{p+1}{6}$ and ϵ_α (resp. $\epsilon_{-\alpha}$) is the centrally primitive idempotent in $\mathbb{C}\langle A\rangle$ corresponding to $\psi^{(\alpha)}$ (resp. $\psi^{(-\alpha)}$).*

(i) Let $\mathfrak{M}$ be a maximal order of $\mathcal{Q}_{\sqrt{p},\infty,\infty}$ containing a maximal order of the subalgebra $\mathcal{Q}_{\infty,3}$. If $(M,F) = L_{2(p-1),2}(\mathfrak{M})$ is unimodular, then $(T, \frac{1}{\alpha}F)$ is isometric to the even unimodular lattice of dimension 8. If $\wp$ is a totally positive prime element over p in the maximal order of the endomorphism algebra $End(SL_2(p) \circ \tilde{S}_3) \cong \mathbb{Q}[\sqrt{p}]$ then the rescaled lattice $(T, \frac{\wp}{\alpha}F)$ is p-modular of minimum ≥ 4.

(ii) If $(M,F) = L_{2(p-1),6}$, then $(T, \frac{1}{\alpha}F)$ is isometric to A_2^2. If $(M, \frac{1}{p}F) = L^{\#}_{2(p-1),6}$, then $(T, \frac{1}{p\alpha}F)$ is isometric to A_2^2.

Proof: Using the character tables given in [21] one calculates

$$(\Theta_i)_{|\langle A\rangle} = 2 \sum_{\beta=0,\ \beta\equiv i \pmod 2}^{p} \psi^{(\beta)} - \psi^{(i)} - \psi^{(p+1-i)},$$

where Θ_i is the character of $SL_2(p)$ described in section 2.

In case (i), the restriction of the natural character to $SL_2(p)$ is $2\Theta_{\frac{p+1}{2}} = 2(\Theta + \Theta')$ and in case (ii) it is $2\Theta_\alpha$, hence $\mathsf{dim}(T) = 8$ resp. 4.

To derive the index of $T \oplus T^\perp$ in M, let q be a prime and q^a the largest q-power dividing $p+1$. If $a = 0$, then $\mathbb{Z}_qT$ is a direct summand of $\mathbb{Z}_qM$. Therefore assume that $a \geq 1$. Let R and $N := N_{SL_2(p)}(\langle A\rangle)$ be as in Lemma 4.2. In case (i) the lattice M and its sublattice T can be viewed as $\mathbb{Z}[\frac{1+\sqrt{p}}{2}]$-modules of rank $p-1$ resp. 4. In case (ii) the lattices M and T have a structure over a maximal order of $\mathcal{Q}_{\infty,3}$ and hence over $\mathbb{Z}[\sqrt{-1}]$. In particular for $q = 3$ $\mathbb{Z}_3M$ is regarded as $RSL_2(p)$-module of R-rank $p-1$ via an embedding $R \hookrightarrow End_{\mathbb{Z}_3M}(SL_2(p))$.

First let $q = 2$. Since α and $\frac{p+1}{2} = 3\alpha$ are odd, the character $\psi_{2\alpha}$, which is the only other Frobenius character in the block of $\mathbb{Z}_2N$ containing ψ_α, does not occur in the restriction of Θ_α or $\Theta_{\frac{p+1}{2}}$ to N. Therefore $\mathbb{Z}_2T$ is a direct summand of $\mathbb{Z}_2M$ and 2 does not divide the index $[M : (T \oplus T^\perp)]$.

Now let $q > 2$. A defect group of the block of Θ_α as well as the one of the block containing Θ and Θ' in $RSL_2(p)$ is the Sylow q-subgroup $C_{q^a} \cong D \leq \langle A\rangle$ and has normalizer N. Since N is also the normalizer of the simple subgroup $C_q \leq D$, [8, Lemma (VII.1.5)] states that the RN-module $\mathbb{Z}_qM$ decomposes as

$$\mathbb{Z}_qM_{|RN} = \tilde{M} \oplus P$$

where P is a projective RN-module and the number of indecomposable direct summands of the RN-module $\tilde{M}$ equals the number of indecomposable direct summands of the $RSL_2(p)$-module $\mathbb{Z}_qM$.

If $q > 3$ then in both cases the character afforded by the $\mathbb{Q}_qN$-module $\mathbb{Q}_q\tilde{M}$ does not contain ψ_α. Therefore $\mathbb{Z}_qT$ is a $\mathbb{Z}_qN$-sublattice of P. Lemma 4.2 (i) now implies that in both cases (i) and (ii) the Sylow q-subgroup of $M/(T \oplus T^\perp)$

is $(\mathbb{Z}/q^a\mathbb{Z})^{\mathsf{dim}(T)}$, which is also the Sylow q-subgroup of $T^{\#,F}/T$, because q does not divide the determinant of (M,F).

Now let $q=3$. The character afforded by the $\mathbb{Q}_3[\sqrt{p}]SL_2(p)$-module $\mathbb{Q}_3M$ is 2Θ (or $2\Theta'$) in case (i) and it is Θ_α in case (ii). Hence the one of the $\mathbb{Q}_3[\sqrt{p}]N$-module $\mathbb{Q}_3\tilde{M}$ is $2\sum_{s=1}^{a}\Psi_{\alpha/3^{s-1}}$ in case (i) and it is $\psi+\psi'+\sum_{s=2}^{a}\Psi_{\alpha/3^{s-1}}$ in case (ii) where $\Psi_{\alpha/3^{s-1}}$ is as defined in the proof of Lemma 4.2 (ii).

The $RSL_2(p)$-module $\mathbb{Z}_3M$ is decomposable in case (i). The Green correspondent (cf. e.g. [6, Theorem (20.6)]) of an indecomposable summand of $\mathbb{Z}_3M$ is one of the two isomorphic indecomposable summands $\tilde{M}'$ of $\tilde{M}$. With the notation introduced in Lemma 4.2 (ii) the RN-module $\tilde{M}'$ is isomorphic to $(1-e-e')P_1$, where P_1 is a projective indecomposable Λ-module. Since $\mathbb{Z}_3T$ is a sublattice of $\tilde{M}$, Lemma 4.2 (ii) shows that the Sylow 3-subgroup of $M/(T\oplus T^\perp)$ is $(\mathbb{Z}_3[\sqrt{p}]/3^{a-1}\mathbb{Z}_3[\sqrt{p}])^4\cong(\mathbb{Z}/3^{a-1}\mathbb{Z})^8$.

In case (ii) the character ψ_α only occurs in the character afforded by the projective RN-lattice P. Lemma 4.2 (ii) yields that the Sylow 3-subgroup of $M/(T\oplus T^\perp)$ is $(\mathbb{Z}_3[\sqrt{-1}]/3^a\mathbb{Z}_3[\sqrt{-1}])\oplus(\mathbb{Z}_3[\sqrt{-1}]/3^{a-1}\mathbb{Z}_3[\sqrt{-1}])\cong(\mathbb{Z}/3^a\mathbb{Z})^2\oplus(\mathbb{Z}/3^{a-1}\mathbb{Z})^2$.

The image of $N\circ\tilde{S}_3$ acting on T is the central product $\bar{N}:=\tilde{S}_3\circ\tilde{S}_3$.

In case (ii), this group $\bar{N}$ fixes only one lattice of determinant 3^2 and dimension 4. To determine the p-part of the determinant the explicit description of the irreducible p-modular representations of $SL_2(p)$ as the space of homogenous polynomials of degree s in two variables $\mathbb{F}_p[x,y]_s$, with character β_{s+1} (cf. Lemma 2.3) is used. Extending scalars one may choose a basis $(x^iy^j\mid i+j=s)$ of $\mathbb{F}_{p^2}[x,y]_s$ such that the action of A is $x^iy^jA=\zeta^{(i-j)}x^iy^j$. Hence the character $\psi^{(\alpha)}$ (and hence $\psi^{(-\alpha)}$) occurs in β_{s+1} if and only if there are integers $0\le i,j\le s$ with $i+j=s$ and $i-j=\alpha$, i.e. $\alpha\le s$ and $s\equiv\alpha\pmod 2$. In particular $\psi^{(\alpha)}$ and $\psi^{(-\alpha)}$ do not occur in $\beta_{\alpha-1}$. Since G acts on $L^{\#}_{2(p-1),6}/L_{2(p-1),6}$ with character $2\beta_{\alpha-1}$, one has $(T,\frac{1}{\alpha}F)\cong A_2^2$ if $(M,F)=L_{2(p-1),6}$ and $(T,\frac{1}{p\alpha}F)\cong A_2^2$ if $(M,\frac{1}{p}F)=L^{\#}_{2(p-1),6}$.

Since the trivial 2-modular constituent does not occur in the representation of $\bar{N}$ on $\mathbb{Q}T$, the rescaled primitive lattice $(T,\frac{1}{\alpha}F)$ is even. Hence in the case (i) ($(M,F)=L_{2(p-1),2}(\mathfrak{M})$), it is isometric to E_8, the unique even unimodular lattice of dimension 8. The rescaled lattice $(M,\wp F)$ can be viewed as a unimodular lattice over $\mathfrak{M}$. In particular the rescaled lattice $(T,\frac{\wp}{\alpha}F)$ comes from an even unimodular $\mathbb{Z}[\frac{1+\sqrt{p}}{2}]$-lattice and is therefore of minimum ≥ 4. □

To state the corresponding result for $p\equiv -1\pmod{12}$ the notation for finite rational matrix groups and their lattices as defined in [17, Proposition (II.4)] are used.

The groups $PSL_2(p)\overset{2(3)}{\boxtimes}D_{12}$ and $PSL_2(p)\overset{2(3)}{\otimes}D_{12}\le GL_{2(p-1)}(\mathbb{Q})$ are extensions of $PSL_2(p)\times D_{12}$ by an automorphism of order 2 acting on both direct factors,

where the restriction of the natural character to $PSL_2(p)$ is $2\Theta_{\frac{p+1}{2}}$ in the first case and $2\Theta_{\frac{p+1}{6}}$ in the second case. The corresponding lattices $A_{p-1}^{(\frac{p+1}{4})}\overset{2(3)}{\boxtimes}A_2$ resp. $\hat{A}_{p-1}^{(\frac{p+1}{12})}\overset{2(3)}{\otimes}A_2$ (or $A_{10}\overset{2(3)}{\otimes}A_2$ if $p=11$) contain the tensor product $A_{p-1}^{(\frac{p+1}{4})}\otimes A_2$ resp. $\hat{A}_{p-1}^{(\frac{p+1}{12})}\otimes A_2$ (or $A_{10}\otimes A_2$ if $p=11$) of index $3^{\frac{p-1}{2}}$ cf. [17, Chapter V].

Lemma 4.4 *Let $p\equiv -1 \pmod{12}$ and (M,F) be a primitive lattice of dimension $2(p-1)$ with $(PSL_2(p)\otimes D_{12}).2 \le Aut(M,F)$. Using the notation of Lemma 4.2 and 4.3 let $T := (\epsilon_\alpha+\epsilon_{-\alpha})M\cap M \le M$*

(i) If $(M,F)=A_{p-1}^{(\frac{p+1}{4})}\overset{2(3)}{\boxtimes}A_2$ is of determinant p^{p-1}, then $\mathsf{dim}(T)$ is 8. The rescaled lattice $(T,\frac{1}{\alpha}F)$ is p-modular of minimum ≥ 4.

(ii) If $(M,F)=\hat{A}_{p-1}^{(\frac{p+1}{12})}\overset{2(3)}{\otimes}A_2$ (or $A_{10}\overset{2(3)}{\otimes}A_2$ if $p=11$) is of determinant $p^{2(\alpha-1)}$, then $(T,\frac{1}{\alpha}F)$ is isometric to A_2^2. If $(M,\frac{1}{p}F)=\hat{A}_{p-1}^{(\frac{p+1}{12})}\overset{2(3)}{\otimes}A_2^{\#}$ (or $A_{10}\overset{2(3)}{\otimes}A_2^{\#}$ if $p=11$) is the dual lattice, the sublattice $(T,\frac{1}{p\alpha}F)$ is isometric to A_2^2.

Proof: Most of the proof is completely analogous to the one of Lemma 4.3 and need not be repeated. The main difference is the argumentation in the case $q=2$. As in Lemma 4.2 let 2^a be the maximal 2-power dividing $p+1$.
(i) The restriction of the natural character of $Aut(M,F)$ to $PSL_2(p)$ is $2\Theta_{3\alpha} = 2(\Theta+\Theta')$. Let $R := \mathbb{Z}_2[\frac{1+\sqrt{-p}}{2}]$ if $p\equiv 3 \pmod 8$ and $R:=\mathbb{Z}_2$ if $p\equiv -1 \pmod 8$. Let M' be an indecomposable summand of the $RPSL_2(p)$-module $\mathbb{Z}_2M$. Since the R-rank of M' is $\frac{p-1}{2}\equiv 1 \pmod 2$, a vertex of M' is the Sylow 2-subgroup D of $\bar{N}$, where $\bar{N}$ is as in Lemma 4.2 (iii). By [6, Theorem (20.6)] $\mathbb{Z}_2M_{|\bar{N}} = \tilde{M}\oplus P$, where P is a sum of indecomposable $R\bar{N}$-lattices with vertex of the form ${}^xD\cap\bar{N}$ where $x\in PSL_2(p)-\bar{N}$. Since ψ_α belongs to a block with defect group $C_{2^{a-1}}$, $\mathbb{Z}_2T$ is an R-sublattice of P.
(a) Assume that $p\equiv 3 \pmod 8$, i.e. $a=2$. If $\mathbb{Z}_2T$ is a direct summand of P then [6, Corollary (20.8)] says that M' and an indecomposable summand of $\mathbb{Z}_2T$ have a common vertex. But ψ_α does not belong to a block of $R\bar{N}$ of maximal defect, so this is a contradiction. The only other Frobenius character in the block of ψ_α of $R\bar{N}$ is $\psi_{2\alpha}$. So $\mathbb{Z}_2T$, not being a direct summand of P, is a sublattice of a projective $R\bar{N}$ sublattice of P. Now Lemma 4.2 (iii) implies (i).
(b) Assume that $p\equiv -1 \pmod 8$, i.e. $a>2$. then $C_{2^{a-1}}\cong C\trianglelefteq D$ is a characteristic subgroup of D. Since $\bar{N}=N_{PSL_2(p)}(C)$, C is not of the form ${}^xD\cap\bar{N}$ for some $x\in PSL_2(p)-\bar{N}$. Now $\bar{N}$ is also the normalizer of the simple subgroup $C_2\le C$, hence by [8, Lemma (VII.1.4)] the indecomposable $\mathbb{Z}_2\bar{N}$-modules belonging to blocks with defect group C have either a vertex C

or are projective. Hence $\mathbb{Z}_2 T$ is a sublattice of a projective $\mathbb{Z}_2\bar{N}$-submodule of P and one gets (i) with Lemma 4.2 (iii).

To get the minimum of the lattice $(T, \frac{1}{\alpha}F)$ one has to view it as unimodular $\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$-lattice $\tilde{T}$. If the minimum of $(T, \frac{1}{\alpha}F)$ is 2, this lattice $\tilde{T}$ represents 1. Since the action of the normalizer $N_G(\langle A\rangle)$ on $\tilde{T}$ is irreducible (with image containing ${}^{\pm}S_3 \otimes S_3$) $\tilde{T}$ contains 4 linearly independent vectors of length 1 and hence is isometric to $\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]^4$. But then $Aut(T,F) = C_2 \wr S_4$ does not contain $S_3 \times S_3$, which is a contradiction.
(ii) The block of $\mathbb{Z}_2 PSL_2(p)$ containing Θ_α is of defect 2^{a-1} and has defect group $C_{2^{a-1}}$. As in Lemma 4.3 for $q \geq 5$, one gets that $\mathbb{Z}_2 T$ is a sublattice of a projective $\mathbb{Z}_2\bar{N}$-module. Hence by Lemma 4.2 (iii) the Sylow 2-subgroup of $M/(T \oplus T^\perp)$ is $(\mathbb{Z}/2^{a-1}\mathbb{Z})^4$. The rest is as in the proof of Lemma 4.3. □

We now finish the proof of Theorem 4.1:

Corollary 4.5 *The restriction of the representation Δ of $G := U_2(\mathbb{F}_{p^2})$ on $\mathbb{Q}L$ to the subgroup $SL_2(p)$ has character $2\Theta_{\frac{p+1}{6}}$. The lattice L has determinant $p^{(p-5)/3}$, so $L = E(K)$*

Proof: As seen in the beginning of the proof of Theorem 4.1 the image $\Delta(G)$ is $SL_2(p) : 2 \times C_3$ if $p \equiv 5 \pmod{12}$ and ${}^{\pm}PSL_2(p).2 \times C_3$ if $p \equiv -1 \pmod{12}$. An element $g \in G - (G' \cdot Z(G))$ can be chosen as $g := \begin{pmatrix} 0 & 1 \\ -\zeta^3 & 0 \end{pmatrix}$. The square $g^2 \in core(U)$ lies in the kernel of the action if $\frac{p+1}{2}$ is odd and $-g^2 \in core(U)$ if $\frac{p+1}{2}$ is even. In both cases there is a central subgroup $\langle\omega\rangle \leq Z(\Delta(G)) \subseteq End(\Delta(G))$ with $\omega^2 + \omega + 1 = 0$. Since the values of the characters Θ_i of degree $p-1$ of $SL_2(p)$ are real, the restriction of Δ to $SL_2(p)$ has character $2\Theta_i$ where $i \in \{\frac{p+1}{2}, \frac{p+1}{4}, \frac{p+1}{3}, \frac{p+1}{6}\} \cap \mathbb{Z}$ has the same parity as $\frac{p+1}{2}$ (cf. section 2). The characters $\Theta_{\frac{p+1}{4}}$ and $\Theta_{\frac{p+1}{3}}$ therefore only have to be considered if $p \equiv -1 \pmod{12}$. They extend to the non-split extension ${}^{\pm}PSL_2(p).2$ with character field $\mathbb{Q}[\sqrt{-2}]$ and $\mathbb{Q}[\sqrt{-1}]$ (cf. [21]) contradicting that ω commutes with $\Delta(G)$.

Hence the character of Δ is one of $2\Theta_{\frac{p+1}{2}}$ or $2\Theta_{\frac{p+1}{6}}$.

To apply Lemma 4.3 resp. 4.4 note that there is an additional automorphism $f \in Aut(L)$ defined by $(-(at+b)^{(p+1)/3}, (ct+d)^{(p+1)/2})f := (-(a^p t + b^p)^{(p+1)/3}, (c^p t + d^p)^{(p+1)/2})$. Clearly f maps the set S into itself and fixes the condition (gen) and the numbers of solutions of $(\star)$. Hence $f \in Aut(L)$. The element $f_1 := \Delta(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix})f \in Aut(L)$ centralizes $\Delta(SL_2(p))$ and induces the outer automorphism on the center $Z(\Delta(G)) \cong C_6$. Moreover $f_1^2 = \Delta(-I)$. Hence $H := \langle\Delta(G), f\rangle$ is isomorphic to $(SL_2(p) \circ \tilde{S}_3).2$ if $p \equiv 5 \pmod{12}$

and $H = (PSL_2(p) \otimes D_{12}).2$ if $p \equiv -1 \pmod{12}$. In all four cases H is an absolutely irreducible subgroup of $GL_{2(p-1)}(\mathbb{Q})$ and the H-invariant primitive lattices are isometric to M or $M^\#$, where M is as in Lemma 4.3 resp. 4.4.

Since the lattice $L = \langle S \rangle$ is a sublattice of $E(K)$, L is integral and its determinant is divisible by p.

Assume now that the restriction of Δ to $SL_2(p)$ has character $2\Theta_{\frac{p+1}{2}}$. Then L is isometric to ${}^{(\wp m)}L_{2(p-1),2}(\mathfrak{M})$ resp. ${}^{(m)}\hat{A}_{p-1}^{(\frac{p+1}{4})} \overset{2(3)}{\boxtimes} A_2$ for some totally positive $m \in \mathbb{Z}[\frac{1+\sqrt{p}}{2}]$ resp. $m \in \mathbb{Z}_{>0}$ as described in Lemma 4.3 (i) resp. 4.4 (i). Therefore the lattice $X \cong {}^{(\frac{p+1}{6})}A_2^2$ (defined just before Lemma 4.2) is a sublattice of the lattice $(T, \wp mF)$ resp. (T, mF) (of Lemma 4.3 (i) resp. 4.4 (i)) of minimum $\geq 4\frac{p+1}{6}$. Since the minimum of X is $\frac{p+1}{3}$ this is a contradiction.

Hence $\Delta_{|SL_2(p)}$ has character $2\Theta_{\frac{p+1}{6}}$. Using the parts (ii) of Lemma 4.3 and 4.4 one easily concludes that $(L,h) = L_{2(p-1),6}$ resp. $(L,h) = \hat{A}_{p-1}^{(\frac{p+1}{12})} \overset{2(3)}{\otimes} A_2$ (or $A_{10} \overset{2(3)}{\otimes} A_2$ if $p = 11$) is of determinant $p^{(p-5)/3} = \mathsf{det}(E(K),h)$. Therefore $L = E(K)$. □

Theorem 4.1 and Lemma 4.3 resp. 4.4 yield the following two Corollaries:

Corollary 4.6 *If $p \equiv 5 \pmod{12}$ then $(E(K),h)$ is isometric to $L_{2(p-1),6}$. In particular, the minimum of $L_{2(p-1),6}$ is $\frac{p+1}{3}$. The automorphism group $Aut(L_{2(p-1),6})$ contains the absolutely irreducible subgroup $SL_2(p) \overset{2(3)}{\circ} \tilde{S}_3$.*

In Theorem 2.6 it was also shown, that the subgroup $SL_2(p)$ of the automorphism group of the Mordell-Weil lattice acts on $p+1$ unimodular overlattices of $L_{2(p-1),6}$. It would be nice to see these lattices in $E(K)_{\mathbb{Q}}$ to have an estimation for their minimum.

For $p = 17$ the automorphism group $Aut(L_{32,6}) = SL_2(17) \overset{2(3)}{\circ} \tilde{S}_3$ has two orbits on these 18 lattices of length 12 resp. 6 represented by extremal unimodular lattices L resp. L'. The automorphism group of L is $SL_2(17)$, whereas L' is the Barnes-Wall lattice with automorphism group $2_+^{1+10}.O_{10}^+(2)$.

If $p \equiv -1 \pmod{12}$, ones uses [17, Theorem (V.9)] to show

Corollary 4.7 *If $p \equiv -1 \pmod{12}$ then $(E(K),h)$ is isometric to $\hat{A}_{p-1}^{(\frac{p+1}{12})} \overset{2(3)}{\otimes} A_2$ (resp. $A_{10} \overset{2(3)}{\otimes} A_2$ for $p = 11$) with automorphism group containing $PSL_2(p) \overset{2(3)}{\otimes} D_{12}$.*

For $p = 11$ the lattice $(E(K),h)$ is described in [17, p. 50], because its automorphism group $PSL_2(11) \overset{2(3)}{\otimes} D_{12}$ is a maximal finite subgroup of $GL_{20}(\mathbb{Q})$. It has determinant 11^2 and 12540 vectors of minimal length 4. For $p = 23$ the rank of $E(K)$ is 44. The lattice has determinant 23^6 and 2708112 vectors of minimal length 8.

Remark 4.8 *As pointed out by Elkies, there is a shorter proof of Theorem 4.1 using the elliptic curve* E' : $Y^2 = X^3 + T^p - T$, *which is equivalent to* E *over any extension of* $\mathbb{F}_p$ *that contains elements* ξ, ξ_2, ξ_3, *and* η *with* $\xi^p \neq \xi = \xi^{(p^2)}$, $\xi_2^2 = \xi_3^3 = \xi^p - \xi$, *and* $\eta^{p+1} = -1$ *via the transformation* $T := (\xi t + \xi^p \eta)/(t + \eta)$, $X := \xi_3 x/(t+\eta)^{(p+1)/3}$, *and* $Y := \xi_2 y/(t+\eta)^{(p+1)/2}$.

For $g := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(p)$, $(a, b, c, d \in \mathbb{F}_p, ad - bc = 1)$, *let* $g(T) := (aT + b)/(cT + d)$. *Then the group* $SL_2(p)$ *acts on* $E'(K)$ *via* $(X(T), Y(T)) \cdot g := (X(g(T))/(cT+d)^{(p+1)/3}, Y(g(T))/(cT+d)^{(p+1)/2})$, *since* $g(T)^p - g(T) = (T^p - T)/(cT + d)^{p+1}$.

5 Some lattices constructed with Δ_2.

Let p be a prime $p \equiv 1 \pmod 4$. Consider the matrix group $G := \Delta_2(SL_2(p)) \leq GL_{2(p-1)}(\mathbb{Q})$. Since the representation Δ_2 decomposes into two non equivalent representations over $\mathbb{R}$, $\mathcal{F}(G)$ is of dimension 2 and may be identified with the center $\mathbb{Q}[\sqrt{p}]$ of the endomorphism algebra $C := End(G) \cong \mathcal{Q}_{\sqrt{p},\infty,\infty}$ (cf. Lemma 1.1 (i)). As in Theorem 2.4 let $(L, F) = L_{2(p-1),2}(\mathfrak{M})$ be unimodular. Multiplying F by integral totally positive elements $\alpha \in \mathbb{Z}[\frac{1+\sqrt{p}}{2}] \subseteq C$, one obtains infinitely many integral Euclidean lattices $(L, \alpha F)$.

If $p = 5$, 13, or 17, the class number of the quaternion algebra $\mathcal{Q}_{\sqrt{p},\infty,\infty}$ is one, so G fixes up to isomorphism only the lattice L.

Theorem 5.1 *Let* $p = 5$, 13, *or* 17, *and* $\beta := \frac{5+\sqrt{p}}{2} \in \mathbb{Z}[\frac{1+\sqrt{p}}{2}] =: R \subseteq Z(C)$ *the totally positive generator of* R *with minimal trace. Then the norm* N *of* β *is* $N = 5$, 3, *or* 2 *in the respective cases. Consider the lattices* $L_i := (L, (\beta + i)F)$ *for* $i \in \mathbb{Z}_{\geq 0}$. *Then* L_i *is an even* $(i^2 + 5i + N)$*-modular lattice. The minimum of* L_i *is* $2i + 4$ *if* $p = 5$ *resp.* $4i + 6$ *if* $p = 13$ *or* $p = 17$. *In particular* L_0 *is an extremal* N*-modular lattice. For* $p = 5$, *the lattices* L_i *are the densest lattices in their genus.*

Proof: By Remark 2.4 the normalizer of G in the automorphism group $Aut(L, F)$ of the unimodular lattice contains an element n which induces the Galois automorphism $\bar{}$ on the center $\mathbb{Q}[\sqrt{p}]$ of the endomorphism algebra of G. Therefore one gets for any $0 \neq \alpha \in \mathbb{Q}[\sqrt{p}]$:

$$F^{-1} n(\alpha F) n^{tr} F^{-1} = F^{-1} \bar{\alpha} n F n^{tr} F^{-1} = F^{-1} \bar{\alpha} = (\alpha\bar{\alpha})(\alpha F)^{-1}.$$

So if α is primitive (i.e. $R = \mathbb{Z}[\alpha]$) and totally positive, the lattice $(L, \alpha F)$ is $(\alpha\bar{\alpha})$-modular. To obtain the minimum of L_i consider the unimodular even R-lattice $\mathcal{L} := (L, \pi F)$, where $\pi \in R$ is a totally positive prime element dividing

p, with quadratic form $\phi : \mathcal{L} \times \mathcal{L} \to R$. Then L_i is the $\mathbb{Z}$-lattice with quadratic form $(\beta+i)F = \mathrm{Tr} \circ (\frac{\beta+i}{\pi}\phi)$, where Tr denotes the trace from $\mathbb{Q}[\sqrt{p}]$ to $\mathbb{Q}$.

Assume first that $p = 5$. Then $\beta = \pi = \frac{5+\sqrt{5}}{2}$ and $(\beta+i)F = \mathrm{Tr} \circ \frac{1}{10}(10+5i-i\sqrt{5})\phi$. Let $x \in \mathcal{L}$ with $\phi(x,x) = a+b\sqrt{5}$. Then $x^{tr}(\beta+i)Fx = \mathrm{Tr}(\frac{1}{10}(10+5i-i\sqrt{5})(a+b\sqrt{5})) = 2a+i(a-b)$. Since ϕ is even, one has $a, b \in \mathbb{Z}$ and $a \equiv b \pmod 2$. Moreover the minimum of the $\mathbb{Z}$-lattice L_0 is 4, so $a \geq 2$ and there is $x \in \mathcal{L}$ with $\phi(x,x) = 2$, because 2 is the unique even totally positive element of R with trace 4. Finally $(a+b\sqrt{5})$ is totally positive, therefore $a^2 > 5b^2$. Distinguish 3 cases
If $b \leq 0$, then $2a+i(a-b) \geq a(i+2) \geq 2i+4$, with equality if $(a,b) = (2,0)$.
If $b = 1$, then a is odd and hence $a \geq 3$. Therefore $a-b \geq 2$ and $2a+i(a-b) \geq 2i+6$.
Finally if $b > 1$ then $a-b > (\sqrt{5}-1)b > 1$ and therefore $a-b \geq 2$. Since $a > \sqrt{5}b$ one has $2a+i(a-b) > 2\sqrt{5}b+2i > 4+2i$.

That L_i is the densest lattice in its genus follows from the observation that the Hermite parameter of a (i^2+5i+5)-modular lattice of minimum $\geq 2i+6$ is $\geq (2i+6)/\sqrt{i^2+5i+5} > 2$ contradicting the fact that $E_8 = L_{8,2}(\mathfrak{M})$ is the densest lattice in dimension 8 [3].

Next consider the case $p = 13$. As in the case $p = 5$ one gets that the minimum of L_i is the minimum of $f_i(a,b) := (a-b)+(a-3b)i$, where $a+b\sqrt{13}$ are the values of the quadratic form ϕ on $\mathcal{L}$. Hence $a > \sqrt{13}b > 3.6b$, $a \equiv b \pmod 2$ and $a \geq 6$. If $x \in \mathcal{L}$, then also $\epsilon x \in \mathcal{L}$ for a fundamental unit ϵ of R, one obtains the inequality $\mathrm{Tr}(\epsilon^2(a+b\sqrt{13})) = 11a-39b \geq 12$. With this, one obtains that $\mathsf{min}(f_i(a,b)) \geq 6+6i$ if $b \leq 0$, $\mathsf{min}(f_i(a,b)) \geq 6+4i$ if $b = 1$, and $\mathsf{min}(f_i(a,b)) \geq 8+4i > 6+4i$ for $b \geq 2$.
The integral lattice $(L, \pi F)$ represents 14. Since $Aut(L, \pi F)$ contains an element inducing the Galois automorphism on the center $Z(C)$ the R-lattice $\mathcal{L}$ represents both even totally positive elements $7 \pm \sqrt{13}$ of R with trace 14. So again this minimum is attained because $f_i(7,1) = 6+4i$.

The case $p = 17$ may be dealt with similarly. Here $f_i(a,b) = a-3b+i(2a-8b)$ and it is helpful to compute that the minimum of L_0 is 6 and the one of L_1 is 10 and to use this restriction on the representation numbers of $\mathcal{L}$. In particular $\mathcal{L}$ represents $18+4\sqrt{17}$ so the minimum $f_i(18,4) = 6+4i$ is attained. □

Remark 5.2 *If $p = 29$, 37, or 41 the algebra $\mathcal{Q}_{\sqrt{p},\infty,\infty}$ contains two conjugacy classes of maximal orders (cf. [25]). For $p = 37$ both unimodular lattices $L_{72,2}(\mathfrak{M})$ contain vectors of length 6. For $p = 41$ only one of the two unimodular lattices $L_{80,2}(\mathfrak{M})$, (the one, where $\mathfrak{M}$ contains a maximal order of $\mathcal{Q}_{\infty,3}$), remains a candidate to be extremal. For $p = 29$, 37, and 41 none of the modular lattices ${}^{(\beta)}L_{2(p-1),2}(\mathfrak{M})$ (where $\beta = \frac{7+\sqrt{p}}{2}$) is extremal.*

A further operation one might apply to the lattices $L_{2(p-1),2}(\mathfrak{M})$ is taking tensor products over maximal anti-identifyable subrings O of the endomorphism rings. The automorphism group of this lattice contains a subgroup $\Delta_2(SL_2(p)) \underset{S}{\otimes} \Delta_2(SL_2(q))$, where $S := \mathbb{Q}O$ is the $\mathbb{Q}$-subalgebra spanned by O, isomorphic to the central product of $SL_2(p)$ and $SL_2(q)$. To obtain a unimodular lattice one usually has to choose an appropriate quadratic form in $\mathcal{F}_{>0}(\Delta_2(SL_2(p)) \underset{S}{\otimes} \Delta_2(SL_2(q)))$.

Clearly for $p = q = 5$, $S = \mathcal{Q}_{\sqrt{5},\infty,\infty}$ one again obtains the lattice $L_{8,2}(\mathfrak{M})$, but for $p = 5$, $q = 13$ (where one may take the subalgebra S to be $\mathcal{Q}_{\infty,2}$) one obtains a new extremal unimodular lattice L_{48} of dimension 48.

Choosing $p = 5$, $q = 17$ ($S \cong \mathcal{Q}_{\infty,3}$) one obtains a unimodular lattice (L, F) but also a 3-modular lattice $(L, p_3 F)$ of dimension 64, where p_3 is a totally positive prime element in $\mathbb{Q}[\sqrt{17}, \sqrt{5}]$ dividing 3. Both lattices remain candidates to be extremal *. To show the 3-modularity of $(L, p_3 F)$, one constructs an element $n \in Aut(L, F)$ which induces the Galois automorphism of $\mathbb{Q}[\sqrt{17}, \sqrt{5}]$ over $\mathbb{Q}[\sqrt{17}]$. Since $np_3n^{-1} = (4 + \sqrt{17})^2 p_3^{-1}$, the 3-modularity of $(L, p_3 F)$ can be seen as in the proof of Theorem 5.1.

One might hope to construct an extremal unimodular lattice of dimension 72 with $p = q = 13, S = \mathcal{Q}_{\sqrt{13},\infty,\infty}$, but this lattice contains vectors of length 6.

An easy construction for the extremal unimodular lattice L_{48} in dimension 48 is the following: Let $\mathfrak{M}$ be a maximal order in $\mathcal{Q}_{\sqrt{13},\infty,\infty}$ and F_3 denote a Gram matrix of the extremal 3-modular lattice ${}^{(\frac{5+\sqrt{13}}{2})}L_{24,2}(\mathfrak{M})$. Let $i \in M_{24}(\mathbb{Q})$ be an element of order 4 in the endomorphism ring $End_{L_{24,2}(\mathfrak{M})}(\Delta_2(SL_2(13)))$. Since iF_3 is skew symmetric, one has $i^{tr} = -F_3^{-1} i F_3$ (cf. Lemma 1.1 (ii)). Using this one easily checks that the matrix

$$F := \begin{pmatrix} F_3 & (1+i) \\ (1+i)^{tr} & 3F_3^{-1} \end{pmatrix}$$

is a Gram matrix of a positive definite 48-dimensional unimodular lattice M, where 1 denotes the 24×24 unit matrix. Moreover the group $SL_2(13)$ is a subgroup of the automorphism group $Aut(M)$ via the representation $\Delta_2 + \Delta_2^{-tr}$. One computes (e.g. with PARI), that the minimum of M is 6. The identification of L_{48} with M may be obtained computing the automorphism group of M:

Theorem 5.3 *The lattice M is an extremal even unimodular lattice. $Aut(M)$ contains a subgroup $SL_2(13)$ such that the normalizer $N := N_{Aut(M)}(SL_2(13))$*

*Meanwhile I proved the extremality of the unimodular lattice (L, F)

is the absolutely irreducible group $(SL_2(13) \underset{S}{\otimes} SL_2(5)).2^2$, *where* $S \cong \mathcal{Q}_{\infty,2}$. *In particular* $M = L_{48}$ *is not isometric to one of the two known extremal unimodular lattices* P_{48p} *and* P_{48q} *(cf. [5]) of dimension 48.*

Proof: It remains to compute N. Using only calculations in dimension 24, one may obtain $a \in GL_{24}(\mathbb{Z})$, such that $3aF_3^{-1}a^{tr} = F_3$ and $a(1+i)a^{-1} = (1+i)^{tr}$. Then the matrix $\begin{pmatrix} 0 & a \\ a^{-tr} & 0 \end{pmatrix}$ lies in $Aut(M)$ and induces the outer automorphism on $SL_2(13)$ and the Galois automorphism on the center of the endomorphism algebra $A := End(SL_2(13)) \cong M_2(\mathcal{Q}_{\sqrt{13},\infty,\infty})$. The centralizer $C := C_{Aut(M)}(SL_2(13))$ consists of all elements in the simple algebra A, fixing M and the quadratic form F. Let $0 \neq v \in M$ be any vector. Then $vA \cap M$ is a lattice of rank dividing 32 $(= \mathsf{dim}_{\mathbb{Q}}(A))$. One computes C as the subgroup of $Aut(vA \cap M, F)$ which lies in A as $C \cong SL_2(5).2$. Therefore $N = \langle SL_2(13), a, C\rangle = (SL_2(13) \underset{S}{\otimes} SL_2(5)).2^2$. □

Remark 5.4 *Since the automorphism group* $Aut(M)$ *contains an irreducible subgroup* $\cong C_{65}$, *the lattice* M *has a structure over the* 65*-th cyclotomic field. The existence of many root free unimodular lattices having such a structure has been predicted in [2]. However it is shown in [1] that an extremal unimodular lattice may not be obtained from a principal ideal in* $\mathbb{Z}[\zeta_{65}]$.

References

[1] C. Bachoc and C. Batut, Etude Algorithmique de Réseaux Construits avec la Forme Trace, *Exp. Math.* **1** (1992), 183-190.

[2] E. Bayer-Fluckiger, Definite unimodular lattices having an automorphism of given characteristic polynomial, *Comm. Math. Helvetii* **59** (1984), 509-538.

[3] H.F. Blichfeldt, The minimum values of positive quadratic forms in six, seven and eight variables, *Math. Zeit.* **39** (1935), 1-15.

[4] R. Burkhardt, Die Zerlegungsmatrizen der Gruppen $PSL(2,p^f)$, *J. Algebra* **40** (1976), 75-96.

[5] J.H. Conway and N.J.A. Sloane, "Sphere Packings, Lattices and Groups", Springer-Verlag 1988.

[6] C.W. Curtis and I. Reiner, "Methods of Representation Theory with applications to finite groups and orders", vol. 1, John Wiley and Sons 1981.

[7] L. Dornhoff, "Group representation theory", Part B, Pure and Applied Mathematics, Marcel Dekker 1972.

[8] W. Feit, "The Representation Theory of Finite Groups", North-Holland 1982.

[9] W. Feit, The computations of some Schur indices, *Isr. J. Math.* **46** 4, (1983), 274-300.

[10] B.H. Gross, Group representations and lattices, *J. AMS* **3** (1990), 929-960.

[11] S. Lang, "Introduction to Modular Forms", Grundlehren der mathematischen Wissenschaften 222, Springer-Verlag 1976.

[12] H. Napias, Etude expérimentale et algorithmique de réseaux euclidiens, These 1454, Bordeaux I (1996).

[13] G. Nebe, Finite quaternionic matrix groups, (submitted)

[14] G. Nebe and W. Plesken, "Finite rational matrix groups of degree 16", AMS-Memoirs, vol. 116, No 556 (1995).

[15] C. Batut, D. Bernardi, H. Cohen, and M. Olivier, PARI-GP 1.39, Université Bordeaux I (1995).

[16] W. Plesken, "Group rings of finite groups over the p-adic integers", Springer Lecture Notes in Mathematics **1026** 1983.

[17] W. Plesken and G. Nebe, "Finite rational matrix groups", AMS-Memoirs, vol. 116, No 556 (1995).

[18] W. Plesken, B. Souvignier, Computing isometries of lattices, *J. Symbolic Computation* **24**, No 3/4 (1997), 327-334

[19] H.-G. Quebbemann, Modular lattices in Euclidean Spaces, *J. Number Theory* **54** No. 2 (1995), 190-202.

[20] W. Scharlau, "Quadratic and Hermitian Forms", Grundlehren der mathematischen Wissenschaften 270, Springer-Verlag 1985.

[21] I. Schur, Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, p. 198-250 in I. Schur: *Gesammelte Abhandlungen I.* Springer-Verlag 1973 resp. *J. reine u. angew. Math.* **132** (1907), 85-137.

[22] T. Shioda, Mordell-Weil lattices and Galois Representations, *Proc. Japan Acad.* **65**, Ser. A (1989), 268-271.

[23] T. Shioda, Mordell-Weil lattices and sphere packings, *Amer. J. Math.* **113** (1991), 931-948.

[24] P.H. Tiep, Globally Irreducible Representations of Finite Groups and Integral Lattices *Geometriae Dedicata* **64** (1997), 85-123.

[25] M.-F. Vignéras, "Arithmétique des Algèbres de Quaternions", Springer Lecture Notes in Mathematics **800** 1980.

[26] L.C. Washington, "Introduction to Cyclotomic Fields", Springer Graduate Texts in Mathematics **83** 1982.