Groups-Complexity-Cryptology
Volume 1 (2009), No. 2, 287–295

Existence and Non-Existence of Torsion in Maximal Arithmetic Fuchsian Groups

C. Maclachlan
Department of Mathematical Sciences,
Aberdeen Universiy, Aberdeen, Scotland

Dedicated to Benjamin Fine on the occasion of his 60th birthday.

Received: May 20, 2009

1. Introduction

In [1], Borel discussed discrete arithmetic groups arising from quaternion algebras over number fields with particular reference to arithmetic Kleinian and arithmetic Fuchsian groups. In these cases, he described, in each commensurability class, a class of groups which contains all maximal groups. Developing results on embedding commutative orders of the defining number field into maximal or Eichler orders in the defining quaternion algebra, Chinburg and Friedman [2] stated necessary and sufficient conditions for the existence of torsion in this class of groups in terms of the defining arithmetic data. This was more fully explored in the case of Kleinian groups in [3]. In the case of Fuchsian groups, these results on the existence of torsion were extended to obtain formulas for the number of conjugacy classes of finite cyclic subgroups for each group in this class [8, 9]. In this paper, we examine, across the range of arithmetic Fuchsian groups, how widespread torsion is in maximal Fuchsian groups. Some studies in low genus cases (see e.g. [7, 12]) indicate that 2-torsion is very prevalent. The results obtained here substantiate that but we will also obtain maximal arithmetic Fuchsian groups which are torsion-free. The author is grateful to Alan Reid for conversations on parts of this paper.

2. Arithmetic Fuchsian groups

Let k be a totally real number field and A a quaternion algebra over k. Let k_ν denoted the completion of k at the place ν and set $A_\nu = A \otimes_k k_\nu$, a quaternion algebra over k_ν. The algebra A is said to be *ramified at* ν if A_ν is a division algebra. The set of ramified places, $\mathrm{Ram}(A)$, is finite of even cardinality and is the union of $\mathrm{Ram}_\infty(A)$, the set of real ramified places, and $\mathrm{Ram}_f(A)$, the set of finite or non-Archimedean ramified places, each being defined by a prime ideal $\mathcal{P}$ of k. The isomorphism class of A is determined by k and $\mathrm{Ram}(A)$ and for any totally real field k and finite set of even cardinality of places there exists

ISSN 1867-1144 / $ 2.50

a quaternion algebra over k with that set as its ramified set. [For details on quaternion algebras and subsequent material in this section, see [1, 10, 11].]

For Fuchsian groups we require that A is ramified at all real places except one so that there exists an embedding $\rho : A \to M_2(\mathbb{R})$. An order $\mathcal{O}$ in A is a complete R_k-lattice which is a ring with 1. Let

$$\mathcal{O}^1 = \{\alpha \in \mathcal{O} \mid n(\alpha) = 1\}$$

where n is the (reduced) norm. Then $P(\rho(\mathcal{O}^1))$ is a Fuchsian group of finite co-area and the class of groups commensurable with all such $P(\rho(\mathcal{O}^1))$ is the class of *arithmetic Fuchsian groups*. The commensurability class is independent of the choice of order $\mathcal{O}$ and only depends, up to conjugation, on the isomorphism class of the quaternion algebra. Furthermore, since the commensurator of $P(\rho(\mathcal{O}^1))$ in $\mathrm{PGL}(2, \mathbb{R})$ is $P(\rho(A^*))$, we can drop the reference to the representation ρ and take the *commensurability class* $\mathcal{C}(A)$ to consist of groups in $P(A^*)$ commensurable with $P(\mathcal{O}^1)$.

For $\alpha \in A^*$, $n(\alpha) \in k^*_\infty$, those elements which are positive at all places in $\mathrm{Ram}_\infty(A)$. If, in addition, $P(\alpha)$ lies in a Fuchsian group, then $n(\alpha) > 0$ so that $n(\alpha) \in k^*_+$, the group of totally positive elements.

3. Maximal arithmetic Fuchsian groups

We now describe the family of groups which includes all maximal Fuchsian groups in the commensurability class $\mathcal{C}(A)$ (see [1, 2, 10]). Let $\mathcal{O}$ denote a maximal order in A so that $\mathcal{O}_\mathcal{P} = \mathcal{O} \otimes_{R_k} R_\mathcal{P}$ is a maximal order in $A_\mathcal{P} = A \otimes_k k_\mathcal{P}$. For $\mathcal{P} \in \mathrm{Ram}_f(A)$, $\mathcal{O}_\mathcal{P}$ is the unique maximal order in $A_\mathcal{P}$. Otherwise, $A_\mathcal{P} \cong M_2(k_\mathcal{P})$ and $\mathcal{O}_\mathcal{P} \cong M_2(R_\mathcal{P})$. Furthermore, all maximal orders in $M_2(k_\mathcal{P})$ are conjugates of $M_2(R_\mathcal{P})$ and form the vertices of a tree on which $\mathrm{GL}(2, k_\mathcal{P})$ acts transitively by conjugation. An edge joining two adjacent vertices represented by maximal orders $\mathcal{O}_\mathcal{P}, \mathcal{O}'_\mathcal{P}$ corresponds to an Eichler order $\mathcal{E}_\mathcal{P} = \mathcal{O}_\mathcal{P} \cap \mathcal{O}'_\mathcal{P}$ of level $\mathcal{P}$. If $\mathcal{O}$ and $\mathcal{O}'$ are maximal orders in A, then $\mathcal{E} = \mathcal{O} \cap \mathcal{O}'$ is an *Eichler order of square-free level* S, where S is a finite set of primes disjoint from $\mathrm{Ram}_f(A)$, if, for $\mathcal{P} \notin S$, $\mathcal{O}_\mathcal{P} = \mathcal{O}'_\mathcal{P}$ and for $\mathcal{P} \in S$, $\mathcal{E}_\mathcal{P} = \mathcal{O}_\mathcal{P} \cap \mathcal{O}'_\mathcal{P}$ is an Eichler order of level $\mathcal{P}$.

Let $N(\mathcal{O})$ denote the normaliser of $\mathcal{O}$ in A^* and $N(\mathcal{O})^+$, the subgroup of those elements with totally positive norm. In the same way, define $N(\mathcal{E})^+$ for $\mathcal{E}$ an Eichler order.

Theorem 3.1 (Borel). *Every arithmetic Fuchsian group in $P(A^*)$ is conjugate to a subgroup of some $P(N(\mathcal{O})^+)$ for $\mathcal{O}$ a maximal order or of some $P(N(\mathcal{E})^+)$ for $\mathcal{E}$ an Eichler order of square-free level.*

There are finitely many conjugacy classes of groups $P(N(\mathcal{O})^+)$ in $\mathcal{C}(A)$ and these are the groups of smallest co-area in $\mathcal{C}(A)$. Furthermore, these groups are all maximal.

For $\mathcal{E}$ an Eichler order of square-free level $S \neq \emptyset$, the group $P(N(\mathcal{E})^+)$ may not be maximal. However, there are infinitely many conjugacy classes of maximal arithmetic Fuchsian groups in $\mathcal{C}(A)$. This can be shown as follows: an element $\alpha \in \mathrm{GL}(2, k_{\mathcal{P}})$ is *odd or even* according as $det(\alpha) \in \mathcal{P}^m$ with m odd or not. Odd elements interchange two adjacent vertices in the tree, so that $P(N(\mathcal{E}_{\mathcal{P}}))$, the stabiliser of an edge, contains odd elements while $P(N(\mathcal{O}_{\mathcal{P}}))$, the stabiliser of a vertex, contains only even elements. Then for any $\mathcal{P} \notin \mathrm{Ram}_f(A)$, one can use the Strong Approximation Theorem to construct a group in $\mathcal{C}(A)$ which contains an element which is odd at $\mathcal{P}$. A maximal group containing this group will contain elements which are odd at a finite set of primes including $\mathcal{P}$. Choosing a prime $\mathcal{P}'$ outside this collection one can repeat the construction. The newly constructed group cannot then be conjugate to a subgroup of the maximal group. Thus maximal groups in infinitely many conjugacy classes are obtained.

The above construction can be modified to construct a torsion-free group in $\mathcal{C}(A)$ which is odd at a given prime. Thus, in the class of torsion-free groups in $\mathcal{C}(A)$, there will be infinitely many conjugacy classes of maximal members. (For all this, see [1], [10, Chap. 11]).

4. Torsion in $P(A^*)$

Recall that A is a quaternion algebra over a totally real number field and A is ramified at all real places except one. To simplify some statements, we will also assume that A is a division algebra. This only rules out the familiar case where $A = M_2(\mathbb{Q})$ and $\mathcal{C}(A)$ consists of groups commensurable with the classical modular group $\mathrm{PSL}(2, \mathbb{Z})$.

If there is to be torsion in any group in $\mathcal{C}(A)$, these elements of finite order must lie in $P(A^*)$. For the converse we have

Theorem 4.1. *Let $u \in A^* \setminus k^*$. Then $P(u)$ belongs to a maximal Fuchsian group in $\mathcal{C}(A)$ if and only if $n(u) \in k_+^*$ and $\mathrm{disc}(u)/n(u) \in R_k$ where $\mathrm{disc}(u) = \mathrm{tr}^2(u) - 4n(u)$.*

(For the proof of this and the following material, see [2], [10, Chap. 12]).

Now $P(A^*)$ contains an element of order $m > 2$ if and only if $2\cos 2\pi/m \in k$ and the field $k(\mathrm{e}^{2\pi i/m})$ embeds in A. In that case, there is, up to conjugacy, a unique subgroup of order m in $P(A^*)$ generated by an image of $1 + \mathrm{e}^{2\pi i/m}$. For $u = 1 + \mathrm{e}^{2\pi i/m}$, $n(u) \in k_+^*$ and $\mathrm{disc}(u)/n(u) = -2 + 2\cos 2\pi/m \in R_k$ so such an element always belongs to some maximal Fuchsian group in $\mathcal{C}(A)$.

Elements $P(u)$ of order 2 in $P(A^*)$ are such that $u^2 \in k, u \notin k$. So u is a pure quaternion, $u^2 = -n(u)$ and $L = k(u)$ embeds in A. Thus provided $n(u) \in k_+^*$, then $P(u)$ will lie in some maximal Fuchsian group. So there are elements of order 2 in some maximal Fuchsian group in $\mathcal{C}(A)$ if and only if there exist quadratic extension fields L of k which are totally imaginary and embed in A.

The following classical theorem determines when a quadratic extension field of k can embed in a quaternion algebra over k.

Theorem 4.2. *Let A be a quaternion algebra over the number field k. Let L be a quadratic extension of k. Then L embeds in A if and only if $L \otimes_k k_\nu$ is a field for each place $\nu \in \mathrm{Ram}(A)$.*

Theorem 4.3. *In every commensurability class of arithmetic Fuchsian groups there are infinitely many conjugacy classes of maximal groups which contain elements of order 2.*

Proof. Let $\mathcal{T} = \Omega_\infty \cup \mathrm{Ram}_f(A)$ where Ω_∞ is the set of all real places of k. For $\nu \in \Omega_\infty$, let $L_\nu \cong \mathbb{C}$ and for $\mathcal{P} \in \mathrm{Ram}_f(A)$, let $L_\mathcal{P}$ be the unique unramified quadratic extension of $k_\mathcal{P}$. For $\mathcal{Q}$ a prime ideal not in $\mathrm{Ram}_f(A)$, let $L_\mathcal{Q}$ be such that $\mathrm{disc}(L_\mathcal{Q} \mid k_\mathcal{Q}) \in \pi R^*_\mathcal{Q}$ where π is a uniformiser in $k_\mathcal{Q}$. By the Approximation Theorem, there exists a quadratic extension L of k such that $L \otimes_k k_\nu \cong L_\nu$ for all $\nu \in \mathcal{T} \cup \{\mathcal{Q}\}$. Then L is totally imaginary and embeds in A. Let $L = k(u)$ with $u^2 \in k$ so that $n(u) \in k^*_+$ and $P(u)$ is an element of order 2 which is odd at $\mathcal{Q}$ lying in some maximal group. Then as described in §3, by Borel's argument, there will be infinitely many conjugacy classes of such groups which are maximal. $\square$

This result is not true for any other orders of torsion.

Example 4.4. Let A be defined over $\mathbb{Q}$ with $\mathrm{Ram}_f(A) = \{p, q\}$ where $p \equiv 1 (\mathrm{mod}\ 12)$. The only candidates for finite order elements in $P(A^*)$ are 2,3,4 or 6. There will be elements of order 3 if $\mathbb{Q}(\mathrm{e}^{2\pi i/3}) = \mathbb{Q}(\sqrt{-3})$ embeds in A and there will be elements of order 4 if $\mathbb{Q}(\mathrm{e}^{2\pi i/4}) = \mathbb{Q}(\sqrt{-1})$ embeds in A. But the ideal $p\mathbb{Z}$ splits in both $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-1})$ so that $P(A^*)$ has no torsion other than that of order 2.

On the other hand (cf. [10, Chap. 12])

Theorem 4.5. *For every m, there exist infinitely many commensurability classes of arithmetic Fuchsian groups which contain an element of order m.*

Proof. Let $k_0 = \mathbb{Q}(\cos 2\pi/m)$. Choose $\alpha \in k_0$ to be totally positive and such that $k = k_0(\sqrt{\alpha})$ is a quadratic extension. By Dirichlet's Density Theorem, there are infinitely many primes $\mathcal{P} \in k$ such that $\mathcal{P}$ is inert in $L = k(\mathrm{e}^{2\pi i/m})$. Let A be defined over k, be ramified at all real places except one and $\mathrm{Ram}_f(A) = \{\mathcal{P}\}$. Then L embeds in A and some maximal Fuchsian group in $\mathcal{C}(A)$ has an element of order m. $\square$

5. Torsion in $P(N(\mathcal{E})^+)$

We now consider more specifically torsion in the groups $P(N(\mathcal{E})^+)$. Here $\mathcal{E}$ is an Eichler order of square-free level S and we will allow $S = \emptyset$, in which case, $\mathcal{E} = \mathcal{O}$ a maximal order. For this we require the following notation.

In the ideal group I_k, let $\mathcal{D}$ denote the subgroup generated by all prime ideals in $\mathrm{Ram}_f(A)$, let $\mathcal{S}$ denote the subgroup generated by all $\mathcal{P} \in S$ and I_k^2 the subgroup generated by all squares of ideals. Also P_k will be the subgroup of principal ideals and $P_{k,+}$ those with a generator in k_+^*.

If we define $H(S) = \{n(\alpha) \mid \alpha \in N(\mathcal{E})^+\}$ then ([9])

$$H(S) = \{x \in k_+^* \mid xR_k \in \mathcal{DS}I_k^2\}.$$

Chinburg and Friedman [2] gave necessary and sufficient conditions for an element $u \in A^*$ to be such that a conjugate of $P(u)$ lies in $P(N(\mathcal{E})^+)$. Applying this to $u = 1 + \mathrm{e}^{2\pi i/m}$, $m > 2$ and combining with Theorem 4.2 on embedding $k(u)$ in A we have

m**-torsion:** $P(N(\mathcal{E})^+)$ has an element of order m if and only if all the following conditions hold

a) $2\cos 2\pi/m \in k$.
b) No $\mathcal{P} \in \mathrm{Ram}_f(A)$ splits in $L = k(\mathrm{e}^{2\pi i/m})$.
c) $(2 + 2\cos 2\pi/m)R_k \in \mathcal{DS}I_k^2$.
d) For each $\mathcal{P} \in S$, at least one of the following conditions must hold:
  - $(2 + 2\cos 2\pi/m)$ is odd at $\mathcal{P}$.
  - $\mathcal{P}$ splits in L.
  - $\mathcal{P} \mid (2 - 2\cos 2\pi/m)R_k$.

An element $P(u)$ of order 2 in $P(N(\mathcal{E})^+)$ has $u^2 = -n(u)$ with $n(u) \in H(S)$. As $P(u)$ is only defined up to scalar multiples of u, $n(u)$ only depends on the element of the finite group $F(S) = H(S)/k^{*2}$. Thus in this case we have:

2-torsion: $P(N(\mathcal{E})^+)$ has an element of order 2 if and only if for some $n \in F(S)$, the following two conditions hold:

a) No prime $\mathcal{P} \in \mathrm{Ram}_f(A)$ splits in $L = k(\sqrt{-n})$.
b) For each $\mathcal{P} \in S$ at least one of the following conditions must hold:
  - n is odd at $\mathcal{P}$.
  - $\mathcal{P}$ splits in L.
  - $\mathcal{P} \mid 4R_k$.

Note that the last conditions in m-torsion and 2-torsion are vacuous when $\mathcal{E} = \mathcal{O}$, a maximal order.

We also note that $P(N(\mathcal{E})^+)$ will indeed be maximal (see §3) if there is no proper subset S' of S such that

$$P_{k,+} \cap \mathcal{DS}I_k^2 = P_{k,+} \cap \mathcal{DS}'I_k^2.$$

For all this see [9].

Theorem 5.1. *Every maximal arithmetic Fuchsian group defined over $\mathbb{Q}$ has 2-torsion.*

Proof. Let A be defined over $\mathbb{Q}$ with $\mathrm{Ram}_f(A) = \{p_1, p_2, \ldots, p_{2r}\}$ and $S = \{q_1, q_2, \ldots, q_s\}$. Then $F(S)$ is represented by the positive divisors of $D = \prod_{i=1}^{2r} p_i \prod_{j=1}^{s} q_j$. A divisor $d \mid D$ contributes an element of order 2 if and only if $(-d/p_i) \neq 1$ for all i and for each q_j either $q_j \mid d$, $(-d/q_j) = 1$ or $q_j = 2$.

If $d = D$, then $(-D/p_i) = 0$ for all i and $q_j \mid D$ for all j. Thus there are elements of order 2 from $\mathbb{Q}(\sqrt{-D})$. □

It is obvious, and well-known, that if $\mathrm{Ram}_f(A) = \emptyset$, then $P(N(\mathcal{O})^+)$, for $\mathcal{O}$ a maximal order, has 2- and 3-torsion. Here we extend that slightly.

Theorem 5.2. *If* $\mathrm{Ram}_f(A) = \emptyset$ *and* $|S| \leq 2$, *then every maximal group* $P(N(\mathcal{E})^+)$ *where* $\mathcal{E}$ *is an Eichler order of level* S *has torsion.*

Proof. If $|S| = 1$ and $P(N(\mathcal{E})^+)$ is maximal, then $P_{k,+} \cap \mathcal{S}I_k^2 \neq P_{k,+} \cap I_k^2$. So there exists $x \in k_+^*$ such that x is odd at $\mathcal{P}$ where $S = \{\mathcal{P}\}$. So $x \in H(S)$ and contributes an element of order 2. If $|S| = 2$ and $P(N(\mathcal{E})^+)$ is maximal, then there exist elements in k_+^* which are odd at $\mathcal{P}_1$ and ones which are odd at $\mathcal{P}_2$ where $S = \{\mathcal{P}_1, \mathcal{P}_2\}$. But then there must exist at least one element which is odd at both $\mathcal{P}_1$ and $\mathcal{P}_2$, thus contributing an element of order 2. □

6. Torsion-free maximal arithmetic Fuchsian groups

Using the results of the preceding section, we show here how to construct families of torsion-free maximal arithmetic Fuchsian groups and give some specific examples (cf. [3]).

Let k be a totally real field with $[k : \mathbb{Q}]$ odd. Furthermore choose k so that it does not contain $\mathbb{Q}(\cos 2\pi/m)$ for any m apart from $m = 2, 3, 4$ or 6. Thus we need only consider 2-and 3-torsion. We will choose $\mathrm{Ram}_f(A) = \{\mathcal{P}_1, \mathcal{P}_2\}$ with the choice of $\mathcal{P}_2$ depending on the choice of $\mathcal{P}_1$.

Now suppose in addition that k has odd class number and even narrow class number. Then corresponding to an order 2 subgroup of $I_k/P_{k,+}I_k^2$ there is a class field M which is a quadratic extension of k with $M \mid k$ having no finite ramification and real ramification at a non-zero set of real places of k. In fact the real ramification will be at an even number of places since the product of the local Artin symbols for $M \mid k$ at the global idele -1 is 1 and is also $(-1)^r$ where r is the number of real ramified places e.g. [6]. Note that, if a prime ideal $\mathcal{P}$ of k is such that $\Phi_{M|k}(\mathcal{P})$ is non-trivial in $\mathrm{Gal}(M \mid k)$ where $\Phi_{M|k}$ is the Artin map, then $\mathcal{P}$ will be inert in M.

Choose $\mathcal{P}_1 = x_1 R_k$ where $x_1 \in k_+^*$.

Let F be the subgroup of k^* defined by

$$F = \{x \in k^* \mid x \text{ is totally positive or totally negative and } xR_k \in \mathcal{D}_1 I_k^2\}$$

where $\mathcal{D}_1 = \langle \mathcal{P}_1 \rangle$. Then $F \supset k^{*2}$ and F/k^{*2} is a finite group. So we have a Kummer extension $L = k(\{\sqrt{x} : x \in F\})$. Let $L' = L(\sqrt{-3})$. Then any quadratic extension of k which is contained in L' is of the form $k(\sqrt{x})$ or $k(\sqrt{-3x})$, $x \in F$ and so is either totally real or totally imaginary. In particular, $M \not\subset L'$.

Let K be the Galois closure of M and L' over k. Choose $\sigma \in \mathrm{Gal}(K \mid k)$ so that $\sigma|_M \neq Id$ and $\sigma|_{L'} = Id$. Then by Tchebotarev's Density Theorem, we can choose a prime $\mathcal{P}_2$ of k which is inert in M and splits completely in L'.

Let $\mathrm{Ram}_f(A) = \{\mathcal{P}_1, \mathcal{P}_2\}$. Elements of order 2 in $P(N(\mathcal{O})^+)$ for $\mathcal{O}$ a maximal order arise from those elements $n \in H = \{x \in k_+^* \mid xR_k \in \mathcal{D}I_k^2\}$ such that $\mathcal{P}_1$ and $\mathcal{P}_2$ do not split in $k(\sqrt{-n})$. Now if $n \in H$, then n, and hence $-n$, belongs to F. For suppose $nR_k = \mathcal{P}_1^t\mathcal{P}_2J^2$. Then $\mathcal{P}_2 = nx_1^{-t}R_kJ^{-2} \in P_{k,+}I_k^2$ and $\Phi_{M|k}(\mathcal{P}_2) = Id$. But this is false by construction. So $-n \in F$ and by construction $\mathcal{P}_2$ splits in $k(\sqrt{-n})$. Thus $P(N(\mathcal{O})^+)$ has no elements of order 2. In the same way, $P(N(\mathcal{O})^+)$ has no elements of order 3 since $\mathcal{P}_2$ splits in $k(\sqrt{-3})$. Thus $P(N(\mathcal{O})^+)$ is torsion-free.

Note that, for each field k satisfying the initial criteria, there are infinitely many choices for $\mathcal{P}_1$ and infinitely many for $\mathcal{P}_2$. Thus there are infinitely many commensurability classes of arithmetic Fuchsian groups defined over k with each $P(N(\mathcal{O})^+)$, for $\mathcal{O}$ a maximal order, torsion-free.

Example 6.1. Let $k = \mathbb{Q}(x)$ where $x^3 - 4x - 1 = 0$. This field has class number 1 and since $[R_{k,+}^* : R_k^{*2}] = 2$, has narrow class number 2. Note that $\Delta_k = 229$. Choose $\mathcal{P}_1 = 3R_k$. In this case we have $M = k(\sqrt{x})$ since x is a fundamental unit with signs $+ - -$. We then require to find an ideal $\mathcal{P}_2$ which is inert in M but splits completely in the field generated by $\sqrt{-1}, \sqrt{x+2}, \sqrt{3}$ over k since $x+2$ is a totally positive unit. Note from the co-area formula for $P(N(\mathcal{O})^+)$ [1, 10], that

$$\mathrm{Co-area\ of\ } P(N(\mathcal{O})^+) = 2\pi \frac{4\zeta_k(2)\Delta_k^{3/2}}{(4\pi^2)^3} \frac{(27-1)(N\mathcal{P}_2 - 1)}{4} = 2\pi 2(g-1).$$

Computing $\zeta_k(2)$ quite precisely, with the help of PARI [4], we find that the rational $(4\zeta_k(2)\Delta_k^{3/2})/(4\pi^2)^3$ is equal to $1/3$. So $N\mathcal{P}_2 - 1 \equiv 0 (\mathrm{mod}\ 12)$. Again making use of PARI, we search for primes $\mathcal{P}_2$ satisfying the required conditions. One possibility is $\mathcal{P}_2 = (3x+2)R_k$ where $N\mathcal{P}_2 = 37$ so giving that $P(N(\mathcal{O})^+)$ has signature $(40; -)$. Another is $\mathcal{P}_2 = (4x^2 + 4x - 1)R_k$ so $N\mathcal{P}_2 = 241$ and $P(N(\mathcal{O})^+)$ has signature $(261; -)$.

The method above can readily be extended to obtain torsion-free maximal groups of the form $P(N(\mathcal{E})^+)$ where $\mathcal{E}$ is an Eichler order of level $S \neq \emptyset$, as we now show.

Choose the field k as above and also $\mathcal{P}_1 = x_1R_k$ with $x_1 \in k_+^*$. Now also choose a prime ideal $\mathcal{Q} = yR_k$ with $y \in k_+^*$ and $(\mathcal{Q}, \mathcal{P}_1) = 1$. Define F similarily to above except with $\mathcal{D}_1 = \langle \mathcal{P}_1, \mathcal{Q} \rangle$. As before we can find a prime $\mathcal{P}_2$ which is inert in M and splits completely in the Kummer extension extended by $\sqrt{-3}$. Note that the first condition a) in 2-torsion fails so there will be no elements of order 2 and likewise no elements of order 3. Thus for $\mathcal{E}$ of level $S = \{\mathcal{Q}\}$, $P(N(\mathcal{E})^+)$ is torsion-free. Note that, since $\mathcal{Q} \in P_{k,+} \cap \mathcal{D}\mathcal{S}I_k^2$, $P(N(\mathcal{E})^+)$ is indeed a maximal group. In these cases, $P(N(\mathcal{O})^+)$ will also be torsion-free.

One essential feature of the above class of examples is that the degree $[k:\mathbb{Q}]$ is odd. This ensures that the class field M, which has an even number of real ramified places, is not a subfield of the Kummer extension. This can also be achieved when the degree is even and we give an example.

Example 6.2. Take $k = \mathbb{Q}(\sqrt{4+\sqrt{5}})$ so that $[k:\mathbb{Q}] = 4$ and k is totally real with $\Delta_k = 4400$ and class number 1. The narrow class number is 2 as $[R^*_{k,+} : R^{*2}_k] = 2$. As before, let M be the class field for the group $I_k/P_{k,+}I_k^2$.

Note in this case that $\mathbb{Q}(\sqrt{5}) \subset k$ and so there could be elements of prime orders 2,3 or 5 in $P(N(\mathcal{O})^+)$. Thus slightly modifying our construction we choose $F = \{x \in k^* \mid x$ is totally positive or totally negative and $xR_k \in \mathcal{T}I_k^2\}$ where $\mathcal{T}$ is the subgroup of I_k generated by $3R_k$ and $\sqrt{5}R_k$. Now F/k^{*2} has order 16 with generators given by $-1, u, 3, (5+\sqrt{5})/2$ where u is a totally positive fundamental unit. Let K be the Kummer extension of k corresponding to the subgroup F of k^* so that every quadratic extension of k in K has the form $k(\sqrt{t})$ for t taken to lie in F/k^{*2}. If t is divisible by 3, then $3R_k$ divides tR_k to an odd power and so is ramified in $k(\sqrt{t})$ by Hilbert's Theorem on relative quadratic extensions [5]. If t is divisible by $(5+\sqrt{5})/2$, then, since $\sqrt{5}R_k$ is the product of two prime ideals of norm 5, $k(\sqrt{t})$ is ramified at a prime of norm 5 over k. If t is not divisible by 3 or $(5+\sqrt{5})/2$ then, up to squares, $t = -1, u, -u$. Note that $2R_k = \mathcal{P}_4^2$. With the help of PARI, we find that $\mathcal{P}_4$ is ramified in the extensions $k(\sqrt{-1}), k(\sqrt{u}), k(\sqrt{-u})$. So all quadratic extensions of k contained in K have finite ramification.

Thus M is not contained in K and by the same argument as before there will be primes in k which are inert in M and split completely in K. Thus choosing $\mathrm{Ram}_f(A) = \{\mathcal{P}\}$ for any such prime, will show that $P(N(\mathcal{O})^+)$ is torsion-free.

For a specific example, we note that $M = k(\sqrt{v})$ for some unit v. The group R_k^*/R_k^{*2} has order 16 with generators obtained from $-1, u_1, u_2, u_3$ where $u_1 = (1+\sqrt{5})/2$, $u_2 = \alpha + (3+\sqrt{5})/2$, $u_3 = \alpha(-1+\sqrt{5})/2 - 2$ where $\alpha = \sqrt{4+\sqrt{5}}$. Again we use PARI to consider the fields $k(\sqrt{v})$ where v is a unit and find that only the field $k(\sqrt{-u_1})$ has no finite ramification over k. Thus M will be $k(\sqrt{-u_1})$.

In this case we calculate that the rational $4\zeta_k(2)\Delta^{3/2}/(4\pi^2)^4$ is equal to 17/30 so that the co-area of $P(N(\mathcal{O})^+) = 2\pi(17/60)(N\mathcal{P} - 1)$. Thus $N\mathcal{P} \equiv 1 (\mathrm{mod}\ 120)$. Now $241R_k = \mathcal{P}\mathcal{P}'\mathcal{P}''$ where $N\mathcal{P} = N\mathcal{P}' = 241$ and $N\mathcal{P}'' = 241^2$. Taking $\mathcal{P}$ to be either of the two primes of norm 241, we find that it is inert in M and splits completely in K. This then yields that $P(N(\mathcal{O})^+)$ has signature $(35; -)$.

References

[1] A. Borel: Commensurability classes and volumes of hyperbolic 3-manifolds, Ann. Sc. Norm. Super. Pisa, Cl. Sci., IV. Ser. 8 (1981) 1–33.

[2] T. Chinburg, E. Friedman: An embedding theorem for quaternion algebras, J. Lond. Math. Soc., II. Ser. 60 (1999) 33–44.

[3] T. Chinburg, E. Friedman: The finite subgroups of maximal arithmetic subgroups of $PSL(2, \mathbb{C})$, Ann. Inst. Fourier 50 (2000) 1765–1798.

[4] H. Cohen et al.: Freeware, available at http://megrez.math.u-bordeaux.fr .

[5] D. Hilbert: Über die Theorie des relativquadratischen Zahlkörpers, Math. Ann. 51 (1899) 1–127.

[6] G. Janusz: Algebraic Number Fields. 2nd Ed., American Mathematical Society, Providence (1996).

[7] D. Long, C. Maclachlan, A. W. Reid: Arithmetic Fuchsian groups of genus zero, Pure Appl. Math. Q. 2 (2006) 569–599.

[8] C. Maclachlan: Torsion in arithmetic Fuchsian groups, J. Lond. Math. Soc., II. Ser. 73 (2006) 14–30.

[9] C. Maclachlan: Torsion in maximal arithmetic Fuchsian groups, in: Combinatorial Group Theory, Discrete Groups, and Number Theory (Fairfield, 2004; Annandale-on-Hudson, 2005), B. Fine et al. (ed.), Contemporary Mathematics 421, American Mathematical Society, Providence (2006) 213–225.

[10] C. Maclachlan, A. W. Reid: The Arithmetic of Hyperbolic 3-Manifolds, Graduate Texts in Mathematics 219, Springer, New York (2003).

[11] M.-F. Vignéras: Arithmétique des Algèbres de Quaternions, Lecture Notes in Mathematics 800, Springer, Berlin (1980).

[12] J. Voight: Shimura curves of genus at most two, Math. Comput. 78 (2009) 1155–1172.