pp. 392–399 in: *ANTS Proceedings 1998*, Buhler (ed.), LNCS 1423, Springer-Verlag 1998.

# Generating Arithmetically Equivalent Number Fields with Elliptic Curves

Bart de Smit

Rijksuniversiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands

**Abstract.** In this note we address the question whether for a given prime number $p$, the zeta-function of a number field always determines the $p$-part of its class number. The answer is known to be no for $p = 2$. Using torsion points on elliptic curves we give for each odd prime $p$ an explicit family of pairs of non-isomorphic number fields of degree $2p + 2$ which have the same zeta-function and which satisfy a necessary condition for the fields to have distinct $p$-class numbers. By computing class numbers of fields in this family for $p = 3$ we find examples of fields with the same zeta-function whose class numbers differ by a factor 3.

## 1 Introduction

Two fields are said to be *arithmetically equivalent* if they have the same zeta-function. The easiest examples of non-isomorphic arithmetically equivalent fields are the fields $K = \mathbb{Q}(\sqrt[8]{a})$ and $K' = \mathbb{Q}(\sqrt[8]{16a})$, where $a$ is any integer for which both $|a|$ and $2|a|$ are not squares. One can show that the class number quotient $h(K)/h(K')$ is 1 or 2 or 1/2; see [4]. By actually computing the class numbers for some small $a$ one finds that all three values occur [5]. The question we will address in this paper is the following.

> *For a given odd prime number $p$, do there exist arithmetically equivalent number fields for which the $p$-parts of the class numbers are distinct?*

We expect the answer to be yes for all $p$. In this paper we will construct, for each prime $p > 2$, a family of pairs of fields of degree $2p+2$ which have the same zeta-function but which also satisfy a necessary condition for the class numbers to have distinct $p$-parts. By computing class groups of some fields in the family for $p = 3$ of relatively small discriminant, we found examples which settle the question in the affirmative for $p = 3$.

To find examples for larger $p$ by this method will require a considerable amount of computation with class groups or units of fields of degree at least 12. We hope that the families of fields given in this paper will provide interesting testing material for those working on improving the performance of software for computing class groups and units.

In Section 2 we will describe the necessary combinatorial conditions that the Galois groups of arithmetically equivalent fields have to satisfy in order to have any hope that they may have distinct $p$-parts of the class numbers. Since we want

pp. 392–399 in: *ANTS Proceedings 1998*, Buhler (ed.), LNCS 1423, Springer-Verlag 1998.

to compute class numbers, we want our fields to have small degree. The smallest degree for which we could produce the right combinatorial setting is $2p+2$. For $p = 3$, 5 and 7 we know that this degree is minimal. Since our construction is based on the group $G = \mathrm{GL}_2(\mathbb{F}_p)$, we can find our fields in any Galois extensions of $\mathbb{Q}$ with Galois group $\mathrm{GL}_2(\mathbb{F}_p)$.

It is well known that the group $\mathrm{GL}_2(\mathbb{F}_p)$ can be realized as a Galois group over $\mathbb{Q}$ by adjoining the coordinates of $p$-torsion points of an elliptic curve. These torsion points are described by explicit division polynomials. In Section 3 we show how one can produce the equations for our particular subfields. We can control the discriminant of the fields we obtain by starting with an elliptic curve with small conductor.

In Section 4 we address the issue of deciding when two arithmetically equivalent fields have the same $p$-class number, and we give a small table of results for $p = 3$.

## 2 Group theoretic setting

Let $N$ be a finite Galois extension of $\mathbb{Q}$ with Galois group $G$. By Galois theory, the category of fields that can be embedded in $N$ is anti-equivalent to the category of transitive $G$-sets $X$. Under this equivalence a field $K$ corresponds to the set of field embeddings of $K$ in $N$. By the formalism of the Artin $L$-function, two such fields have the same zeta-function if and only if for the corresponding $G$-sets $X$ and $X'$ we have an isomorphism of $\mathbb{C}[G]$-modules $\mathbb{C}[X] \cong \mathbb{C}[X']$; see [2] This last condition is also equivalent to the $\mathbb{Q}[G]$-modules $\mathbb{Q}[X]$ and $\mathbb{Q}[X']$ being isomorphic (cf. [2, p. 110]).

One can show that the two number fields must have isomorphic $p$-parts of the class group if we have a $\mathbb{Z}_p[G]$-module isomorphism $\mathbb{Z}_p[X] \cong \mathbb{Z}_p[X']$; see [8], [9]. We sketch a short proof: if $C_N$ is the idele class group of $N$, and $U_N$ denotes the group of ideles which are units at the finite primes, then we have a canonical map $f\colon U_N \to C_N$. For a subgroup $H$ of $G$ we have $U_N^H = U_{N^H}$ and $C_N^H = C_{N^H}$. The $p$-part of the class group of $N^H$ is the cokernel of the map that we get by applying the functor $\mathrm{Hom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[G/H], \mathbb{Z}_p \otimes_{\mathbb{Z}} -)$ to $f$, so it depends only on the field $N$ and the $\mathbb{Z}_p[G]$-module $\mathbb{Z}_p[G/H]$.

Thus, our first, purely combinatorial, task is to find for given $p$, a finite group $G$ and two transitive $G$-sets $X$ and $X'$ of smallest cardinality possible so that

$$(*) \qquad \mathbb{Q}[X] \cong_{\mathbb{Q}[G]} \mathbb{Q}[X'] \quad \text{but} \quad \mathbb{Z}_p[X] \ncong_{\mathbb{Z}_p[G]} \mathbb{Z}_p[X'] \ .$$

The key to our construction is to consider the standard action of the group $G = \mathrm{GL}_2(\mathbb{F}_p)$ on the set $V$ of column vectors of length 2 over $\mathbb{F}_p$. Let $V^* = \mathrm{Hom}(V, \mathbb{F}_p)$ be the dual of $V$ with $G$-action given by $(g\varphi)(x) = \varphi(g^{-1}x)$ for $g \in G$, $x \in V$ and $\varphi \in V^*$. The character of the representation $\mathbb{C}[V]$ of $G$ assigns to each element $g \in G$ the number of points of $V$ fixed under $g$. For $g \in G$ the number of fix-points in $V$ and $V^*$ are the same, so it follows that

pp. 392–399 in: *ANTS Proceedings 1998*, Buhler (ed.), LNCS 1423, Springer-Verlag 1998.

$\mathbb{C}[V] \cong_{\mathbb{C}[G]} \mathbb{C}[V^*]$. Taking out the trivial representation, i.e., the zero-elements of $V$ and $V^*$ and changing scalars we get

$$\mathbb{Q}[V\backslash\{0\}] \cong_{\mathbb{Q}[G]} \mathbb{Q}[V^*\backslash\{0\}] \ .$$

Note that the $G$-sets $V\backslash\{0\}$ and $V^*\backslash\{0\}$ are transitive of order $p^2-1$. If $p>2$ then the stabilizer of a point fixes no element of $V^*\backslash\{0\}$, so that the $G$-sets are not isomorphic. Thus, the $G$-sets give non-isomorphic arithmetically equivalent fields. The degree of these fields is the cardinality of $V\backslash\{0\}$, which is $p^2-1$.

Note that the group $\mathbb{F}_p^*$ is embedded in $G$ as the scalar multiplications on $V$. To find fields of smaller degree we consider the action of subgroups $S$ of $\mathbb{F}_p^*$. Since $S$ lies in the center of $G$, we have a quotient $G$-set $X/S$ for any $G$-set $X$. We now consider $X = (V\backslash\{0\})/S$ and $X' = (V^*\backslash\{0\})/S$. We can also take the quotient by $S$ for $G$-modules, so

$$\mathbb{Q}[X] \cong_{\mathbb{Q}[G]} \mathbb{Q}[V\backslash\{0\}]/S \cong_{\mathbb{Q}[G]} \mathbb{Q}[V^*\backslash\{0\}]/S \cong_{\mathbb{Q}[G]} \mathbb{Q}[X'] \ .$$

The stabilizers of elements of $X$ are the conjugates of the subgroup $H = \left(\begin{smallmatrix} S & * \\ 0 & * \end{smallmatrix}\right)$ of $G$, and the stabilizers of the elements of $X'$ are the conjugates of the subgroup $H' = \left(\begin{smallmatrix} * & * \\ 0 & S \end{smallmatrix}\right)$. Note that both $H$ and $H'$ have only one stable 1-dimensional subspace of $V$. If $S \neq \mathbb{F}_p^*$ then the number orbits of $H$ and $H'$ on their stable lines is not the same, so that $X$ and $X'$ are not isomorphic as $G$-sets. For $p>2$ and $S = \mathbb{F}_p^{*2}$ we thus obtain non-isomorphic arithmetically equivalent fields of degree $2p+2$.

In order to check that $\mathbb{Z}_p[X] \ncong_{\mathbb{Z}_p[G]} \mathbb{Z}_p[X']$ we consider the subgroup $H = \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$ of $G$. Note that the $H$ has orbit lengths 1, 1, $2p$ on $X$ and 2, $p$, $p$ on $X'$. This implies that the $\mathbb{Z}_p[G]$-modules $\mathbb{Z}_p[X]$ and $\mathbb{Z}_p[X']$ have distinct Tate-cohomology groups $\hat{H}^0(H,-)$, where $\hat{H}^0(H,M) = M^H/(\sum_{h\in H} h)M$.

This completes the group-theoretic part of the construction. One can summarize as follows:

**Proposition 1.** *Suppose $p$ is an odd prime number. Let $G = \mathrm{GL}_2(\mathbb{F}_p)$, and let $H$ and $H'$ be the subgroups $\left(\begin{smallmatrix} \square & * \\ 0 & * \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} * & * \\ 0 & \square \end{smallmatrix}\right)$ of $G$, where "$\square$" denotes the condition that the matrix entry be a square. Then $H$ and $H'$ have index $2p+2$ in $G$, and the $G$-sets $X = G/H$ and $X' = G/H'$ satisfy $(*)$.*

For $p = 3$, 5 and 7 we have checked computationally that the degree, i.e., the cardinality of the $G$-sets $X$ and $X'$ in this proposition is minimal by using the classification of transitive groups of degree up to 15. Moreover, for $p = 3$ and for $p = 5$ we know that the configuration in the proposition is the only one with this minimal degree. It would be nice to have a more conceptual proof of these statements which may also say something for larger $p$.

For $p = 2$ our construction fails because then $\mathbb{F}_p^*$ has no strict subgroups. The smallest degree in this case is obtained in the same way by taking $G = \mathrm{GL}_3(\mathbb{F}_2)$ rather than $\mathrm{GL}_2(\mathbb{F}_2)$. This leads to number fields of degree 7 as in [8]. In this case $G$ is the simple group group of order 168, and it is quite some work [6] to realize this group as a Galois group over $\mathbb{Q}$ and find explicit equations [1]. An

pp. 392–399 in: *ANTS Proceedings 1998*, Buhler (ed.), LNCS 1423, Springer-Verlag 1998.

example of such fields with distinct 2-parts of the class numbers has been found by Wieb Bosma and the author:

$$x^7 + 8x^6 + x^5 - 15x^4 + 13x^3 + 8x^2 - 20x + 8$$
$$x^7 + 24x^6 + 194x^5 + 604x^4 + 653x^3 + 816x^2 + 359x + 212 \ .$$

These polynomials define two arithmetically equivalent fields with class numbers 2 and 1 respectively.

## 3 Realization as number fields

It is well known that we can realize the group $\mathrm{GL}(2, \mathbb{F}_p)$ as a Galois group over $\mathbb{Q}$ by considering $p$-torsion points on elliptic curves. Such a Galois extension of $\mathbb{Q}$ always contains a $p$-th root of unity, so the families of fields obtained in this way are somewhat limited.

In this section $E$ denotes an elliptic curve

$$E\colon\ y^2 = x^3 + ax + b, \qquad d = 4a^3 + 27b^2 \neq 0$$

with coefficients $a, b \in \mathbb{Q}$. The set $V = E(\bar{\mathbb{Q}})[p]$ of $p$-torsion points is a vector space of dimension 2 over $\mathbb{F}_p$ on which the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts linearly. This means that we have a group homomorphism

$$\rho\colon\ \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E(\bar{\mathbb{Q}})[p]) \cong \mathrm{GL}_2(\mathbb{F}_p) \ .$$

We will *assume* that $a$ and $b$ are chosen in such a way that $\rho$ is surjective. This is true generically (see [10, Rem. 6.7] or [7, Chap. 6, §3]) and by Hilbert's irreducibility theorem the pairs $(a, b)$ for which $\rho$ is not surjective form a "thin" set.

Let us first consider the particularly easy case that $p = 3$. We take $X = V\backslash\{0\}$ and $X' = V^*\backslash\{0\}$. The field corresponding to $X$ is obtained by adjoining both coordinates of a non-trivial 3-torsion point of $E$. Writing $\mu_3$ for the group of third roots of unity in $\bar{\mathbb{Q}}$, we have isomorphisms of Galois representations

$$V^* = \mathrm{Hom}(V, \mathbb{F}_3) \cong \mathrm{Hom}(V, \mu_3) \otimes \mu_3 \cong V \otimes \mu_3 \ .$$

The first isomorphism holds because $\mu_3 \otimes \mu_3$ has trivial Galois action. The second isomorphism is due to the Weil-pairing [11, Chap. 3, §8]. It follows that we get $V^*$ as a Galois representation by twisting $V$ with the quadratic character associated with of the number field $\mathbb{Q}(\mu_3) = \mathbb{Q}(\sqrt{-3})$. But it is also possible to twist the entire elliptic curve by a quadratic character, that is, we have

$$V \otimes \mu_3 \cong E'(\bar{\mathbb{Q}})[3],$$

where $E'$ is the twist of $E$ given by

$$E' : -3y^2 = x^3 + ax + b \ .$$

pp. 392–399 in: *ANTS Proceedings 1998*, Buhler (ed.), LNCS 1423, Springer-Verlag 1998.

Thus, the number field corresponding to $X'$ is obtained by adjoining the coordinates of a non-trivial 3-torsion point of $E'$.

Let give some explicit equations for in this case: the $x$-coordinates of the nontrivial 3-torsion points of $E$ are the four zeros of the division polynomial (see [11, Ex. 3.7])

$$P(x) = 3x^4 + 6ax^2 + 12bx - a^2 \ .$$

By our hypothesis that $\rho$ is surjective, the 4-dimensional $\mathbb{Q}$-algebra $\mathbb{Q}[x]/(P)$ is a field. A purely formal computation shows that the minimum polynomial of the image of $x^3 + ax + b$ in $\mathbb{Q}[x]/(P)$ is

$$f(t) = t^4 + 8bt^3 + \frac{2}{3}dt^2 - \frac{1}{27}d^2 \ .$$

This means that the $y$-coordinates of the nontrivial 3-torsion points of $E$ are the zeros of the octic polynomial $f(t^2) \in \mathbb{Q}[t]$. By considering the isomorphism over $\mathbb{Q}(\sqrt{-3})$ from $E'$ to $E$ that sends $(x, y)$ to $(x, \sqrt{-3}y)$ one sees that the $y$-coordinates of the non-trivial 3-torsion points of $E'$ are the zeros of $f(-3t^2)$. It turns out that the $x$-coordinate of a non-trivial 3-torsion point of $E$ or $E'$ is contained in the field generated by its $y$-coordinate (this follows from the next proposition). Thus, for $p = 3$ the two arithmetically equivalent fields are the fields $\mathbb{Q}(\sqrt{\alpha})$ and $\mathbb{Q}(\sqrt{-3\alpha})$, where $\alpha$ is a zero of the polynomial $f$.

We will now show how to obtain equations for any odd prime $p$. We will not use the standard equations for $p$-torsion points. Let $\mathbb{Q}(E)$ denote the function field of $E$ over $\mathbb{Q}$. Any rational function $\varphi \in \mathbb{Q}(E)$ gives a map

$$E(\bar{\mathbb{Q}}) \to \mathbb{P}^1(\bar{\mathbb{Q}}) = \bar{\mathbb{Q}} \cup \{\infty\} \ ,$$

which is $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-equivariant. Suppose that we have a function $\varphi \in \mathbb{Q}(E)$ that satisfies the following hypotheses.

(1) $\varphi$ has no poles in $E(\bar{\mathbb{Q}})[p]\backslash\{0\}$;
(2) $\varphi$ is constant on each $\mathbb{F}_p^{*2}$-orbit of $E(\bar{\mathbb{Q}})[p]\backslash\{0\}$;
(3) $\varphi$ is not constant on each $\mathbb{F}_p^{*}$-orbit of $E(\bar{\mathbb{Q}})[p]\backslash\{0\}$.

Let the "quadratic twist" of $\varphi$ be the function $\bar{\varphi} = \varphi \circ [n]$ where $n \in \mathbb{Z}$ is not a square modulo $p$ and $[n]$ denotes multiplication by $n$ on $E$. Note that $\bar{\varphi}$ does not depend on the choice of $n$. We now set $\psi = (\varphi - \bar{\varphi})^2$. Let the groups $H$, $H'$ and $G = \mathrm{GL}_2(\mathbb{F}_p)$ be as in Proposition 1.

**Proposition 2.** *Let $p^* = \pm p \equiv 1 \bmod 4$, and let $\alpha = \psi(P) \in \bar{\mathbb{Q}}$ for a non-trivial $p$-torsion point $P \in E(\bar{\mathbb{Q}})$. Then the fields $\mathbb{Q}(\sqrt{\alpha})$ and $\mathbb{Q}(\sqrt{p^*\alpha})$ are the fields of invariants of $H$ and $H'$ in a Galois extension of $\mathbb{Q}$ with Galois group isomorphic to $G$.*

*Proof.* The function $\varphi$ restricts to a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-equivariant map

$$\varphi : \quad E(\bar{\mathbb{Q}})[p]\backslash\{0\} \ \to \ \bar{\mathbb{Q}} \ .$$

pp. 392–399 in: *ANTS Proceedings 1998*, Buhler (ed.), LNCS 1423, Springer-Verlag 1998.

Choose an $\mathbb{F}_p$-basis for $E(\bar{\mathbb{Q}})[p]$ with $P$ as the first basis element. Since the homomorphism $\rho$ is surjective, the image of $\varphi$ lies in a Galois extension $N$ of $\mathbb{Q}$ within $\bar{\mathbb{Q}}$ whose Galois group is identified with $\mathrm{Aut}(E(\bar{\mathbb{Q}})[p]) = \mathrm{GL}_2(\mathbb{F}_p) = G$. Moreover, $\varphi(P)$ is fixed by the subgroup $\left(\begin{smallmatrix}1 & *\\ 0 & *\end{smallmatrix}\right)$ of $G$.

The element $\beta = \varphi(P) - \bar{\varphi}(P) \in \bar{\mathbb{Q}}$ also lies in $N$. A diagonal matrix $M = \left(\begin{smallmatrix}a & *\\ 0 & b\end{smallmatrix}\right) \in G$ now sends $\beta$ to $(\frac{a}{p})\beta$, where $(\frac{a}{p})$ denotes the quadratic symbol. By the Weil-pairing the composite map

$$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho} G \xrightarrow{\det} \mathbb{F}_p^*$$

is equal to the restriction map to $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) = \mathbb{F}_p^*$, where $\mu_p$ denotes the group of $p$-th roots of unity in $\bar{\mathbb{Q}}$. Thus, the matrix $M$ sends $\sqrt{p^*}$ to $(\frac{ab}{p})\sqrt{p^*}$. This implies that $\beta$ is fixed by the subgroup $\left(\begin{smallmatrix}\square & *\\ 0 & *\end{smallmatrix}\right)$ of $G$, and that $\beta\sqrt{p^*}$ is fixed by $\left(\begin{smallmatrix}* & *\\ 0 & \square\end{smallmatrix}\right)$.

It remains to show that $\beta$ and $\beta\sqrt{p^*}$ are not fixed by larger subgroups, because we then know that the fields $\mathbb{Q}(\beta)$ and $\mathbb{Q}(\beta\sqrt{p^*})$ are non-isomorphic and arithmetically equivalent by Proposition 1. Thus, we must show that $\mathbb{Q}(\beta)$ and $\mathbb{Q}(\beta\sqrt{p^*})$ have degree $2p+2$.

We first claim that $\mathbb{Q}(\beta)$ contains no abelian extension of $\mathbb{Q}$ of degree at least 2. To see this, note that the commutator subgroup of $G$ is $\mathrm{SL}_2(\mathbb{F}_p)$, and that the group $\left(\begin{smallmatrix}\square & *\\ 0 & *\end{smallmatrix}\right)$ maps surjectively to $\mathbb{F}_p^*$ by the determinant. We have $\beta \neq 0$ by hypothesis (3) above, and since $-\beta$ is conjugate to $\beta$, it follows that the degree of $\mathbb{Q}(\beta)$ is larger than 2. Thus, the field $\mathbb{Q}(\alpha)$ where $\alpha = \beta^2$ is a nontrivial extension of $\mathbb{Q}$. The element $\alpha$ is fixed by the maximal subgroup $B = \left(\begin{smallmatrix}* & *\\ 0 & *\end{smallmatrix}\right)$ of $G$. Since $\mathbb{Q}(\alpha) \neq \mathbb{Q}$ it follows that $\mathbb{Q}(\alpha)$ has degree $p+1$. We already saw that $B$ does not fix $\beta$, or $\beta\sqrt{p^*}$, so these algebraic numbers have have degree $2p+2$. This proves the proposition.

There are some obvious candidates for the function $\varphi$ above. If $p \equiv -1 \bmod 4$ then we can take $\varphi = \sum_n y \circ [n]$ where $n$ ranges over a set of representatives in $\mathbb{Z}$ of $\mathbb{F}_p^{*2}$. In this case we have $\bar{\varphi} = -\varphi$, and $\psi = 4\varphi^2$. If $p \equiv 1 \bmod 4$ then $-1$ is a square in $\mathbb{F}_p$, and we take $\varphi = \sum_n x \circ [n]$ where $n$ ranges over a set of representatives in $\mathbb{Z}$ of $\mathbb{F}_p^{*2}/\langle -1\rangle$. In both cases hypotheses (1) and (2) are clearly satisfied.

For given $p$, $a$, and $b$ we would now like to find the minimal polynomial $f \in \mathbb{Q}[t]$ of the element $\alpha = \psi(P)$ of $\bar{\mathbb{Q}}$. To do this, it is convenient to first compute approximations of its complex roots by explicitly computing Weierstrass functions. The Pari program (see [3]) is well suited for this.

For small $p$ one could also use the addition formulas or division polynomials and do formal computations over the field $\mathbb{Q}(a,b)$ with transcendental $a$ and $b$, but typically this will take much more effort. In fact, the best method to compute $f$ as a polynomial with coefficients in the transcendental field $\mathbb{Q}(a,b)$, is to compute the polynomial for enough sample values of $a$ and $b$ and then interpolating.

Let us treat some small cases explicitly. For $p=3$ take $\varphi = y$; for $p=5$ take $\varphi = (x - x\circ[2])/2$, and for $p=7$ take $\varphi = y + y\circ[2] + y\circ[4]$. This gives rise to

pp. 392–399 in: *ANTS Proceedings 1998*, Buhler (ed.), LNCS 1423, Springer-Verlag 1998.

the following polynomials for $\alpha$:

$$\begin{array}{ll} p=3: & f(t) = t^4 + 8\,bt^3 + \frac{2}{3}\,dt^2 - \frac{1}{27}\,d^2 \\ p=5: & f(t) = 5\,t^6 + 12\,at^5 - \frac{5}{2}\,d\,t^3 + \frac{1}{16}\,d^2 \\ p=7: & f(t) = 7\,t^8 + 13824\,bt^7 + 51586416\,dbt^5 + 319956\,dt^6 \\ & \quad -42\,d(6237547\,d - 4976640\,b^2)t^4 + 10947369888\,d^2bt^3 \\ & \quad -28\,(150387289\,d + 4417425072\,b^2)d^2t^2 \\ & \quad +226800\,\left(409637\,d + 1174176\,b^2\right)bd^2t \\ & \quad -81\,d^2(17161\,d - 41472\,b^2)^2. \end{array}$$

Here we use the notation $d = 4a^3 + 27b^2$. These "generic" minimal polynomials can be used as follows.

If for given $a$, $b \in \mathbb{Q}$ with $d \neq 0$ the homomorphism $\rho$ is surjective, and 0 is not a root of $f$, then by Proposition 2 the polynomials $f(t^2)$ and $f(p^*t^2)$ define realizations of the $G$-sets of Proposition 1 as field extensions of $\mathbb{Q}$, so that we indeed obtain non-isomorphic arithmetically equivalent fields.

In practice, we do not test whether $\rho$ is surjective for given $a$ and $b \in \mathbb{Q}$, but we test whether $f(t^2)$ and $f(p^*t^2)$ are irreducible. If this is the case, then the Galois group of the minimal common normal field will be a subgroup of the group $\mathrm{GL}_2(\mathbb{F}_p)/\mathbb{F}_p^{*2}$, which we obtain generically. Then the fields are arithmetically equivalent, because if two $G$-sets give isomorphic permutation representations of $G$, then they also give isomorphic permutation representations of any subgroup of $G$. It is still possible that the fields are isomorphic. However, if we are searching for arithmetically equivalent fields with distinct class numbers, then this is of no concern, since fields with distinct class numbers are certainly not isomorphic, and we do not expect to waste a lot of computing time on the thin set of pairs $(a, b)$ with non-generic behavior.

## 4 Computing class numbers

By explicit computations with the equations of the last section, we can answer the question in the introduction for $p = 3$.

**Proposition 3.** *There exist two number fields with the same zeta-function for which the* 3*-parts of the class numbers are distinct.*

To find such fields we used the Pari program. We computed the class numbers of 819 pairs of fields of relatively small discriminant. Of those pairs, 118 had one or both class numbers divisible by 3, and 88 pairs had distinct class numbers. In all these 88 cases the class numbers differed by a factor 3, and one can actually prove that this is the only possibility [1]. We did not use the rigorous version of the routines for class number computation, but we did check correctness of the class number quotients for all 819 pairs by the method given in [5].

In the next table one finds a small selection of these fields with the notation of Section 3: the $a$ and $b$ give the elliptic curve $E$ and its twist $E'$, and the number $D$ is the absolute value of the discriminant of the number fields $K$ and

pp. 392–399 in: *ANTS Proceedings 1998*, Buhler (ed.), LNCS 1423, Springer-Verlag 1998.

$K'$ that one gets by adjoining a non-trivial 3-torsion point of $E$ and $E'$. The class numbers of $K$ and $K'$ are denoted by $h$ and $h'$

| $a$ | $b$ | $D$ | $h$ | $h'$ |
|---|---|---|---|---|
| 12 | 64 | $2^{18}\,3^3\,17^4$ | 1 | 3 |
| 6 | 8 | $2^{22}\,3^{11}$ | 12 | 4 |
| $-51$ | 78 | $3^7\,53^4$ | 3 | 1 |
| 6 | $-3$ | $2^{10}\,3^7\,41^4$ | 3 | 1 |
| $-24$ | $-60$ | $2^4\,3^7\,97^4$ | 1 | 3 |
| 48 | 48 | $2^8\,3^7\,73^4$ | 2 | 6 |

Since it seems unlikely, by the Cohen-Lenstra heuristics, that a degree 12 number field has class number divisible by 5, one would have to sieve through many pairs before finding arithmetically equivalent fields whose class numbers differ by a factor 5. But perhaps this is feasible as routines for class group computations become faster. A theoretical construction which forces a factor 5 in the class number would be even more helpful.

## References

1. Bosma, W., De Smit, B.: On arithmetically equivalent fields of small degree. (in preparation)
2. Cassels, J.W.S., Fröhlich, A. (eds.): Algebraic number theory. Academic Press, London-New York 1967
3. Cohen, H.: A course in computational number theory. Springer-Verlag New York 1993
4. De Smit, B.: On Brauer relations for $S$-class numbers. Technical Report 97-10 Universiteit van Amsterdam 1997
5. De Smit, B., Perlis, R.: Zeta functions do not determine class numbers. Bull. Amer. Math. Soc. **31** (1994) 213–215
6. LaMacchia, S.E.: Polynomials with Galois group PSL$(2,7)$. Comm. Algebra **8** (1980) 983–982
7. Lang, S.: Elliptic functions. Springer-Verlag, New York 1987
8. Perlis, R.: On the class numbers of arithmetically equivalent fields. J. Number Theory **10** (1978) 489–509
9. Roggenkamp, K., Scott, L.: Hecke actions on Picard groups. J. Pure Appl. Algebra **26** (1982) 85–100
10. Shimura, G.: Introduction to the arithmetic theory of automorphic functions. Princeton University Press, Princeton 1971
11. Silverman, J.H.: The arithmetic of elliptic curves. Springer-Verlag, New York 1986