KNOT MODULES AND THE NAKANISHI INDEX

C. KEARTON AND S. M. J. WILSON

(Communicated by Ronald A. Fintushel)

Abstract. We examine the structure of the knot module of 9_{38} and show that the Nakanishi index of this knot is 2. The Nakanishi indices of 10_{69} and 10_{101} are also determined by means of the Fox-Smythe row class. Finally, we point out that the Nakanishi index is not additive over knot composition.

1. Introduction

A knot $k$ is a smooth oriented pair $(S^3, S^1)$; two knots are equivalent if there is an orientation preserving diffeomorphism sending one onto the other. A classical invariant of $k$ is $M(k) = H_1(\tilde{K})$, the first homology of the infinite cyclic cover of the exterior of $k$ regarded as a module over $\Lambda = \mathbb{Z}[t, t^{-1}]$. A presentation of $M(k)$ may be obtained by means of the free differential calculus of Fox (see [4, 7]) or via the Seifert matrix (see [7, 10, 12]).

Of course, $M(k)$ has many presentation matrices, but any two are connected by a finite sequence of elementary moves; see [7, Lemma 7.2.1]. Then Nakanishi’s index is defined to be the least integer $m$ such that the module is presented by an $m \times m$ matrix. In [7, Table F.4] there is a list of minimal presentation matrices of knots with index greater than 1; in the case of $9_{38}$ a $2 \times 2$ matrix is given, although it is not certain that this is minimal. We use a Mayer-Vietoris sequence from algebraic K-theory to establish the structure of the knot module; this enables us to show that in fact this matrix is minimal and so the index of $9_{38}$ is 2.

The Nakanishi indices of $10_{69}$ and $10_{101}$ are also shown to be 2, by means of the Fox-Smythe row class. In the case of $10_{69}$ the computer program PARI was used to help determine the row class. PARI was also used in the investigation of $10_{101}$, although in this case our conclusions do not rely on the PARI calculations.

This settles all the knots in [7, Table F.3] for which Nakanishi’s index is listed as unknown, i.e. those knots with less than or equal to 10 crossings.

Finally, we refer to an example of J.A. Hillman to illustrate that the Nakanishi index is not additive over knot composition.
2. THE MODULE STRUCTURE OF \(M(9_{38})\)

In [7, Table F.4] the following presentation matrix of \(M = M(9_{38})\) is given:

\[
A = \begin{pmatrix}
t^2 - t + 1 & t + 1 \\
0 & 5t^2 - 9t + 5
\end{pmatrix}.
\]

We set

\[
f(t) = t^2 - t + 1, \quad g(t) = 5t^2 - 9t + 5,
\]

so that \(A\) corresponds to a presentation with generators \(x, y\) and relations

\[
(2.1) \quad f(t)x + (t + 1)y = 0, \quad g(t)y = 0.
\]

**Lemma 2.1.** Let \(\omega = (1 + \sqrt{-3})/2\), a root of \(f(t)\). Then

\[
M/f(t)M \cong \mathbb{Z}[\omega] = \mathbb{Z}[\omega, \omega^{-1}].
\]

**Proof.** The equality follows from \(\omega^{-1} = \overline{\omega} = 1 - \omega\). From (2.1) we see that \(M/f(t)M\) is presented as a \(\mathbb{Z}[\omega]\)-module with generators \(x, y\) and relations

\[
(\omega + 1)y = 0, \\
(5\omega^2 - 9\omega + 5)y = 0.
\]

But \(\omega^2 - \omega + 1 = 0\) and \(\omega\) is a unit, so this presentation is equivalent to

\[
(2.2) \quad (\omega + 1)y = 0, \\
4y = 0.
\]

Again, \(-(\omega + 1)(\overline{\omega} + 1) + 4 = 1\), so we have

\[
y = 0.
\]

Hence the result. Note moreover that the presentation gives an epimorphism \(\mathbb{Z}[\omega]^2 \to \mathbb{Z}[\omega]\) sending \(x\) to 1 and \(y\) to 0.

**Lemma 2.2.** Let \(\theta = (9 + \sqrt{-19})/10\), a root of \(g(t)\). Then

\[
M/g(t)M \cong \mathbb{Z}[\theta, \theta^{-1}].
\]

**Proof.** From (2.1) we see that \(M/g(t)M\) is presented as a \(\mathbb{Z}[\theta, \theta^{-1}]\)-module with generators \(x, y\) and relation

\[
(\theta^2 - \theta + 1)x + (\theta + 1)y = 0.
\]

But \(\theta - 1 + \theta^{-1} = \frac{9}{5} - 1 = \frac{4}{5}\), so this presentation is equivalent to

\[
\frac{4}{5}\theta x + (\theta + 1)y = 0.
\]

Thus there is a monomorphism \(M/g(t)M \to \mathbb{Z}[\theta, \theta^{-1}]\) sending

\[
x \mapsto \theta + 1, \quad y \mapsto -\frac{4}{5}\theta.
\]

But \((\theta^{-1} + 1)(\theta + 1) = \frac{19}{5}\) and \(\gcd(19, 4) = 1\), so the map is surjective.

**Lemma 2.3.** As \(\Lambda\)-modules,

\[
M/(f(t), g(t))M \cong \mathbb{Z}[\omega]/(4).
\]
Proof. From (2.1) and (2.2) we see that \( M/(f(t), g(t))M \) is presented as a \( \mathbb{Z}[\omega] \)-module with generators \( x, y \) and relations

\[
(\omega + 1)y = 0, \\
4y = 0, \\
g(\omega)x = 0.
\]

Arguing as in Lemma 2.1, and noting that \( g(\omega) = -4\omega \), we see that this presentation is equivalent to

\[
y = 0, \\
4x = 0.
\]

Hence the result.

Essentially the same argument gives the following corollary.

**Corollary 2.4.** There is a ring isomorphism

\[
\Lambda/(f, g) \cong \mathbb{Z}[\omega]/(4).
\]

Let \( \phi = (1 + \sqrt{-19})/2 \) and note that \( \mathbb{Z}[\phi] \) is the ring of integers of \( \mathbb{Q}(\sqrt{-19}) \), which has class number 1, and so \( \mathbb{Z}[\phi] \) is a UFD.

**Lemma 2.5.** (i) \( \mathbb{Z}[\theta, \theta^{-1}] = \mathbb{Z}[\theta, \theta^{-1}]^\times \), (ii) \( \mathbb{Z}[\theta, \theta^{-1}]^\times = \langle -1, \phi, \overline{\phi} \rangle \).

**Proof.** (i) Clearly \( \mathbb{Z}[\phi] \subseteq \mathbb{Z}[\theta, \theta^{-1}] \), and since \( 2 - \theta - \theta^{-1} = \frac{1}{5} \) we have \( \mathbb{Z}\left[\frac{1}{5}, \phi\right] \subseteq \mathbb{Z}[\theta, \theta^{-1}] \). Since \( \theta = (\phi + 4)/5, \mathbb{Z}[\theta, \theta^{-1}] \subseteq \mathbb{Z}\left[\frac{1}{5}, \phi\right] \).

(ii) Note that \( \theta^{-1} = -\theta = 4\phi/5 \), so \( \overline{\phi} = -\phi \) and that \( \phi \overline{\phi} = 5 \).

Thus \( \phi \) is irreducible and hence prime in \( \mathbb{Z}[\phi] \). Moreover, \( \phi, \overline{\phi} \in \mathbb{Z}[\theta, \theta^{-1}]^\times \), so \( \langle -1, \phi, \overline{\phi} \rangle \subseteq \mathbb{Z}[\theta, \theta^{-1}]^\times \).

Let \( \xi \in \mathbb{Z}[\theta, \theta^{-1}]^\times \). Then

\[
\xi = \frac{\sigma}{\overline{\sigma}} \text{ with } \sigma \in \mathbb{Z}[\phi], \\
\frac{1}{\xi} = \frac{\tau}{\overline{\tau}} \text{ with } \tau \in \mathbb{Z}[\phi],
\]

and so

\[
\sigma \tau = 5^{r+s} = (\phi \overline{\phi})^{r+s}.
\]

Since \( \mathbb{Z}[\phi] \) is a UFD with units \( \pm 1 \), \( \sigma = \pm \phi^a \overline{\phi}^b \). Therefore

\[
\xi = \pm \phi^a \overline{\phi}^b \in \langle -1, \phi, \overline{\phi} \rangle.
\]

Now \( \omega \) is a primitive 6th root of unity, and \( \mathbb{Z}[\omega]^\times = \langle \omega \rangle \) has order 6.

Note that we have a cartesian square of rings

\[
\begin{array}{ccc}
\Lambda/(fg) & \longrightarrow & \Lambda/(f) \\
\downarrow & & \downarrow \\
\Lambda/(g) & \longrightarrow & \Lambda/(f, g)
\end{array}
\]
which, using the results above, can be written as

\[
\begin{array}{ccc}
\Lambda/(fg) & \longrightarrow & \mathbb{Z}[\omega] \\
\downarrow & & \downarrow \beta \\
\mathbb{Z}[\theta, \theta^{-1}] & \longrightarrow & \mathbb{Z}[\omega]/(4)
\end{array}
\]  

(2.3)

where \(\beta(\omega) = \omega\), and \(\delta_0(\theta) = \omega\) since both \(\theta\) and \(\omega\) are the image of \(t\). (Here and elsewhere we write plain \(\lambda\) rather than \(\lambda + (4)\) to denote an element of \(\mathbb{Z}[\omega]/(4)\).)

**Lemma 2.6.** \(f(t)M \cap g(t)M = \{0\}\).

**Proof.** Since \(\det A = f(t)g(t)\) we see that \(f(t)g(t)\) annihilates \(M\); indeed

\[f(t)M \subseteq \ker g(t) \quad \text{and} \quad g(t)M \subseteq \ker f(t).\]

Thus \(f(t)M \cap g(t)M\) is killed by the ideal \((f, g) = (f, 4)\). But \(M\) is \(\mathbb{Z}\)-torsion free, being a knot module; hence the result. \(\Box\)

Thus we have a cartesian square

\[
\begin{array}{ccc}
M & \longrightarrow & M/f(t)M \\
\downarrow & & \downarrow \\
M/g(t)M & \longrightarrow & M/(f, g)M
\end{array}
\]

By the results above this can be written as

\[
\begin{array}{ccc}
M & \longrightarrow & \mathbb{Z}[\omega] \\
\gamma & & \downarrow \beta \\
\mathbb{Z}[\theta, \theta^{-1}] & \longrightarrow & \mathbb{Z}[\omega]/(4)
\end{array}
\]  

(2.4)

where the maps are given by

\[
\alpha(x) = 1, \quad \alpha(y) = 0; \quad \gamma(x) = \theta + 1, \quad \gamma(y) = -\frac{4}{5} \theta;
\]

and \(\delta = \delta' \delta_0\) where \(\delta' : \mathbb{Z}[\omega]/(4) \to \mathbb{Z}[\omega]/(4)\) is given by \(\delta'(1) = (\omega + 1)^{-1}\). Note that \(\omega + 1\) is a unit in \(\mathbb{Z}[\omega]/(4)\), for

\[-(\omega + 1)\omega = -\omega^2 - \omega = 1 - 2\omega\]

whose square is 1 in \(\mathbb{Z}[\omega]/(4)\).

The cartesian squares (2.3) and (2.4) are the same except that in (2.4) the lower map has been twisted by \(\delta'\).

It follows from [11 IX Theorem 5.1] that \(M\) is a projective \(\Lambda/(fg)\)-module of rank 1, which is free only if \(\omega + 1 \in \mathbb{Z}[\omega]/(4)\) lies in the image of

\[
\mathbb{Z}[\theta, \theta^{-1}] \otimes \mathbb{Z}[\omega]^\times
\]

in the Mayer-Vietoris sequence in [11 IX Theorem 5.3]. (An alternative reference is [11 Lemma 4.20(v)].) That image is

\[
\delta_0 \left( \mathbb{Z}[\theta, \theta^{-1}] \otimes \mathbb{Z}[\omega]^\times \right) \subseteq \left( \mathbb{Z}[\omega]/(4) \right)^\times.
\]

But \(\delta_0(\delta) = 5\omega - 4 \equiv \omega \pmod{4}\). Thus the total image is just \(\langle \omega \rangle\), whose only element of order 2 is \(-1\). On the other hand, as we have observed, \(1 - 2\omega\) is a unit.
of order 2 in \( \mathbb{Z}[\omega]/(4) \), which therefore cannot be in this image. Hence neither can 
\((\omega + 1)^{-1} = -\omega(1 - 2\omega)^{-1}\).

So \( M \) is not cyclic and it follows that the Nakanishi index of \( 9_{38} \) is 2.

3. The row class of \( 10_{101} \)

If we apply Seifert’s construction [7, p. 47] to the diagram in [7, Table F.1], we find that the Seifert circuits are not nested. The Seifert surface \( V \) so constructed has an obvious basis for \( H_1(V) \), given by the cycles surrounding the four “holes”. Taking these in the order of lower left-hand, top, lower middle and lower right-hand, and orienting each of them in the anti-clockwise direction, we obtain the following as a Seifert matrix for \( 10_{101} \):

\[
U = \begin{pmatrix}
-1 & -1 & 0 & 0 \\
0 & -3 & 1 & 1 \\
0 & 1 & -2 & 1 \\
0 & 1 & 0 & -2
\end{pmatrix}.
\]

Thus \( M(10_{101}) \) is presented by \( tU - U' \):

\[
\begin{pmatrix}
1 - t & -t & 0 & 0 \\
1 & 3 - 3t & t - 1 & t - 1 \\
0 & t - 1 & 2 - 2t & t \\
0 & t - 1 & -1 & 2 - 2t
\end{pmatrix} \sim \begin{pmatrix}
0 & -t - 3(1 - t)^2 & (t - 1)^2 & (t - 1)^2 \\
1 & 3 - 3t & t - 1 & t - 1 \\
0 & t - 1 & 2 - 2t & t \\
0 & t - 1 & -1 & 2 - 2t
\end{pmatrix}
\]

\[
\sim \begin{pmatrix}
-3t^2 + 5t - 3 & (t - 1)^2 & (t - 1)^2 \\
t - 1 & 2(1 - t) & t \\
t - 1 & -1 & 2(1 - t)
\end{pmatrix}
\]

\[
\sim \begin{pmatrix}
-3t^2 + 5t - 3 + (t - 1)^3 & 0 & (t - 1)^2 - 2(t - 1)^3 \\
t - 1 - 2(t - 1)^2 & 0 & t + 4(t - 1)^2 \\
t - 1 & -1 & 2(1 - t)
\end{pmatrix}
\]

\[
\sim \begin{pmatrix}
t^3 - 6t^2 + 8t - 4 & -2t^3 + 7t^2 - 8t + 3 \\
-2t^2 + 5t - 3 & 4t^2 - 7t + 4 \\
-2t^2 + 5t - 3 & 3t - 2
\end{pmatrix}.
\]

Let \( A(t) \) denote the final matrix above. (The corresponding entry in [7, Table F.4] is incorrect, as calculation of its determinant shows.)

The Alexander polynomial is

\[
f(t) = 7t^4 - 21t^3 + 29t^2 - 21t + 7.
\]

Let \( \theta \) be a root of \( f(t) \), \( L = \mathbb{Q}(\theta) \) and \( O_L \) the ring of integers of \( L \). Let \( K = \mathbb{Q}(\sqrt{21}) \), so that \( O_K = \mathbb{Z}[\frac{1 + \sqrt{21}}{2}] \).

Lemma 3.1. \( L \) contains \( K \) and is totally complex. \([L: \mathbb{Q}] = 4\), and \( f(t) \) is irreducible.

Proof. If we put \( y = t + t^{-1} \), then

\[
t^{-2}f(t) = 7y^2 - 21y + 15 = g(y)
\]

with roots \((21 \pm \sqrt{21})/14\). These both lie in the interval \((0, 2)\), so all the roots of \( f(t) \) are non-real, \([\mathbb{Q}[\theta] : \mathbb{Q}] = 4\), and \( f(t) \) is irreducible. \(\square\)
Lemma 3.2. 
\[ \mathbb{Z} \left[ \theta, \theta^{-1} \right] = \mathbb{Z} \left[ \frac{1}{7} 7\theta \right] \subseteq O_L \left[ \frac{1}{7} \right] . \]

Proof. Let \( \eta = \theta + \theta^{-1} \). Then \( g(\eta) = 0 \), so
\[ 7\eta^2 - 21\eta + 15 = 0 , \]
and hence \( \frac{1}{7} \in \mathbb{Z} \left[ \theta, \theta^{-1} \right] \). Moreover,
\[ \theta^{-1} = -\frac{7\theta^3 - 21\theta^2 + 29\theta - 21}{7} \in \mathbb{Z} \left[ \frac{1}{7}, 7\theta \right] \]
which gives the equality. But \( h(x) = 7^3 f \left( \frac{1}{7} \right) \) is the minimum polynomial of \( 7\theta \) over \( \mathbb{Z} \), and \( h(x) \) is monic, so \( 7\theta \in O_L \). This gives the inclusion, which in fact is an equality, although we do not need that here. \( \square \)

Let \( M = L \left( \sqrt{-3} \right) \).

Lemma 3.3. \( M/L \) is unramified at all the finite and infinite primes.

Proof. \( M = L \left( \sqrt{-7} \right) \) also, since \( \sqrt{21} = \sqrt{-3} \sqrt{-7} \). Now the discriminant of \( O_L \left[ (1 + \sqrt{-3})/2 \right] \) over \( O_L \) is \( (3)_{O_L} \), and that of \( O_L \left[ \sqrt{-7} \right] \) is \((28)_{O_L}\), so the discriminant of \( O_M \) over \( O_L \) divides both of these and hence is \( O_L \). By Dedekind’s theorem, [14, Theorem 4-8-14], \( M/L \) is unramified at all the finite primes. By Lemma 3.1 \( L \) is totally complex, so \( M/L \) is unramified at all the infinite primes. \( \square \)

Let \( H \) be the Hilbert class field of \( L \), i.e. the maximal unramified abelian extension of \( L \). Lemma 3.3 shows that \( M \subset H \). (In fact \( M = H \), but we do not need that here.)

Lemma 3.4. The ideal \( P_5 = (5, 7(\theta + 1))_{O_L} \) is non-principal.

Proof. First note that
\[ N_{L/Q} (7\theta + 7) = h(-7) = 7^3 f(-1) = 7^3 \times 5 \times 17 , \]
and so
\[ N \left( P_5 \right) \mid \gcd \left( N_{L/Q} (7\theta + 7), N_{L/Q} (5) \right) = 5 . \]
If \( \alpha \in P_5 \), then \( \alpha = \beta(7\theta + 7) + 5\gamma \) for some \( \beta, \gamma \in O_L \), and so
\[ N_{L/Q}(\alpha) \equiv N_{L/Q} (\beta) N (7\theta + 7) \equiv 0 \mod 5 . \]
Therefore \( P_5 \neq O_L \), so \( N (P_5) = 5 \) and therefore \( P_5 \) is a prime divisor of \((5)_{O_L} \) with \( O_L/P_5 = \mathbb{F}_5 \). Hence the residue field over \( O_L/P_5 \) corresponding to \( M \) is \( \mathbb{F}_5 \left[ \sqrt{-3} \right] = \mathbb{F}_{25} \), a non-trivial extension. Thus the Artin symbol \( \left( \frac{P_5}{M/L} \right) \neq 1 \) and \( P_5 \) is non-principal (see [9, XI §5]). \( \square \)

Lemma 3.5. \( P_5 \mathbb{Z} \left[ \frac{1}{7} \right] \) is non-principal over \( O_L \left[ \frac{1}{7} \right] \).
Proof. First note that \((1 - \theta)^{-1} \in O_L\) and
\[
N_{L/Q} \left( \frac{1}{1 - \theta} \right) = N_{L/Q} (1 - \theta)^{-1} = \left( \frac{f(1)}{7} \right)^{-1} = 7.
\]
Now 7 ramifies in \(K\), in fact \((7)_{O_K} = P^2\) where \(P = ((7 + \sqrt{21})/2)_{O_K}\), so there are either two conjugate prime divisors or one single prime divisor of \((7)_{O_L} = (PO_L)^2\).
One of these must be \((1 - \theta)^{-1} \in O_L\) and so any prime divisor of \((7)_{O_L}\) is principal. Thus the class group of \(O_L\) maps isomorphically onto that of \(O_L \left[ \frac{1}{7} \right] \) and, therefore, since \(P_5\) is non-principal, so is \(P_5O_L \left[ \frac{1}{7} \right] \) (over \(O_L \left[ \frac{1}{7} \right] \)).

The argument in [3] shows that the element of the class group of \(Z[\theta, \theta^{-1}]\) represented by the ideal generated by the \(i^{th}\) row of \(A(\theta)\) is independent of \(i\), and is an invariant, the row class, of the knot.

The row class of \(A(\theta)\) is the ideal class in \(Z[\theta, \theta^{-1}]\) of
\[
I = (-2\theta^2 + 5\theta - 3, 3\theta - 2) = (-2\theta - 3)(\theta - 1), 3\theta - 2)
= (2\theta - 3, 3\theta - 2) = (2\theta - 3, \theta + 1) = (5, \theta + 1)_{Z[\theta, \theta^{-1}]}.
\]
So \(IO_L \left[ \frac{1}{7} \right] = P_5Z \left[ \frac{1}{7} \right] \) is non-principal. Therefore \(I\) is non-principal and so the row class of \(10_{101}\) is non-trivial. But if \(M(10_{101})\) were cyclic, \((f(t))\) and hence \((f(t)^{0})\) would be a presentation matrix. Thus the row class would be trivial. Hence the Nakanishi index of \(10_{101}\) is 2.

4. THE ROW CLASS OF 10\(_{69}\)

In [7, Table F.4] the following presentation matrix of \(M(10_{69})\) is given:
\[
A(t) = \begin{bmatrix}
  t^2 + t - 1 & 3t^3 - 9t^2 + 5t - 1 \\
  2t^2 - 2t + 1 & t^4 - 2t^3
\end{bmatrix}.
\]
The Alexander polynomial is
\[
f(t) = t^6 - 7t^5 + 21t^4 - 29t^3 + 21t^2 - 7t + 1.
\]
The following properties were found by using the computer program PARI:
(i) \(f(t)\) is irreducible, with root \(\theta\) say.
(ii) \(Z[\theta] = Z[\theta, \theta^{-1}]\) is the ring of integers of \(Q[\theta]\).
(iii) The class number of \(Z[\theta]\) is 2.
(iv) The ideal
\[
(2\theta^2 - 2\theta + 1, \theta^4 - 2\theta^3) = (2\theta^2 - 2\theta + 1, \theta - 2) = (5, \theta - 2)
\]

is not principal.
As in the previous section, the Nakanishi index of \(10_{69}\) is 2.

5. NON-ADDITIVITY OF THE NAKANISHI INDEX

First recall from [8] that knot modules have been characterised. Using this, we can deduce from [6, pp. 562-563] that there exist two knots, \(k\) and \(l\), with the following properties:
(i) \(k\) and \(l\) both have Alexander polynomial \(f(t) = 13t^2 - 25t + 13\), which is irreducible.
(ii) $M(k)$ is not cyclic, hence $k$ has Nakanishi index 2. (This is because the degree of the Alexander polynomial is an upper bound for the Nakanishi index, since by [13, pp. 485-489] a knot module can always be presented via a non-singular Seifert matrix.)

(iii) $M(l) \cong \Lambda/(f(t))$, hence $l$ has Nakanishi index 1.

(iv) $M(k + k) \cong M(l + l) \cong \Lambda/(f(t)) \oplus \Lambda/(f(t))$, so $k + k$ has Nakanishi index 2.

It follows that the Nakanishi index is not additive over knot composition.

Of course, we could use $10_69$ or $10_{101}$ in place of $k$, but Hillman’s example is much easier. Another method is to consider two knot polynomials with resultant equal to 1, such as the cyclotomic polynomials $\Phi_6$ and $\Phi_{35}$, so that

$$\Lambda/(\Phi_6\Phi_{35}) \cong \Lambda/(\Phi_6) \oplus \Lambda/(\Phi_{35}).$$

The argument in [6, p. 561] provides two knots $k, l$ with knot modules $\Lambda/(\Phi_6)$, $\Lambda/(\Phi_{35})$ respectively, and then $k + l$ has knot module $\Lambda/(\Phi_6\Phi_{35})$.

6. THE PARI PROGRAM

PARI (more completely, PARI/GP) is a software package implementing many algorithms to do with the arithmetic of algebraic number fields and elliptic curves. Originally developed at Bordeaux by a team led by Henri Cohen, it is now maintained by Karim Belabas at the Université Paris-Sud, Orsay, with the help of many volunteer contributors. The web address of the PARI home page is http://www.parigp-home.de/.

PARI/GP is available under the GNU General Public License. Acquisition of the package (from the above address) is easy, installation is straightforward and the documentation [2] is good. PARI is most easily used via its command line interface, GP. It is not primarily an algebraic manipulation package, although it has a similar feel, and it is extremely powerful in carrying out calculations which few other packages attempt.

PARI/GP is used by many number theorists in their investigations. One might add that the command line interface is necessarily somewhat awkward and technical and the learning curve can be steep!

The principal use of PARI in the present research was to calculate the ideal class groups of the relevant number fields. For this PARI implements the algorithm of Buchmann [3].

REFERENCES


Department of Mathematics, University of Durham, South Road, Durham DH1 3LE, England

E-mail address: Cherry.Kearton@durham.ac.uk

Department of Mathematics, University of Durham, South Road, Durham DH1 3LE, England

E-mail address: S.M.J.Wilson@durham.ac.uk