

Computations on Milnor K_2 of integer rings

Romyar Sharifi

Max Planck Institute of Mathematics

May 17, 2004

Milnor K_2 of integer rings:

F number field, S finite set of primes of F

$\mathcal{O}_{F,S}$ ring of S -integers of F

We define Milnor K_2 of $\mathcal{O}_{F,S}$ as

$$K_2^M(\mathcal{O}_{F,S}) = \frac{\mathcal{O}_{F,S}^\times \otimes_{\mathbf{Z}} \mathcal{O}_{F,S}^\times}{\langle x \otimes (1-x) \mid x, 1-x \in \mathcal{O}_{F,S}^\times \rangle}.$$

For $x, y \in \mathcal{O}_{F,S}^\times$, let $\{x, y\}$ denote the image of $x \otimes y$ in $K_2^M(\mathcal{O}_{F,S})$.

Let $k_v =$ the residue field of F at a prime v .

We have a commutative diagram

$$\begin{array}{ccccccc}
 K_2^M(\mathcal{O}_{F,S}) & \longrightarrow & K_2^M(F) & & & & \\
 \vdots \downarrow & & \parallel & & & & \\
 0 \longrightarrow & K_2(\mathcal{O}_{F,S}) & \longrightarrow & K_2(F) & \longrightarrow & \bigoplus_{v \notin S} k_v^\times & \longrightarrow 0,
 \end{array}$$

where the upper horizontal map is induced by the natural map on symbols and the right-hand lower horizontal map is given by tame symbols. The map $K_2^M(\mathcal{O}_{F,S}) \rightarrow K_2(\mathcal{O}_{F,S})$ given by the natural map on symbols need not be injective/surjective.

Example: $F = \mathbf{Q}(\sqrt{-d})$, $d \geq 5$, d square free

$$\mathcal{O}_{F,\emptyset}^\times = \mathcal{O}_F^\times = \langle -1 \rangle$$

$$K_2^M(\mathcal{O}_F) = \langle \{-1, -1\} \rangle \cong \mathbf{Z}/2\mathbf{Z}$$

For $d = 5$, Tate showed that

$$K_2(\mathcal{O}_F) = 0.$$

For $d = 39$, Browkin-Belabas-Gangl showed that

$$K_2(\mathcal{O}_F) \cong \mathbf{Z}/6\mathbf{Z}.$$

Our focus:

p an odd prime, ζ a primitive p th root of 1

$$F = \mathbf{Q}(\mu_p), S = \{(1 - \zeta)\}, \mathcal{O}_{F,S} = \mathbf{Z}[\frac{1}{p}, \zeta]$$

$\mathcal{C} = \langle 1 - \zeta^i \mid 1 \leq i \leq p - 1 \rangle$ cyclotomic p -units

$$\mathcal{C} \cong \mathbf{Z}^{\oplus(p-1)/2} \oplus \mathbf{Z}/2p\mathbf{Z}$$

$$[\mathcal{O}_{F,S}^\times : \mathcal{C}] = h^+ = \text{class number of } \mathbf{Q}(\zeta + \zeta^{-1})$$

Vandiver's Conjecture. $p \nmid h^+$

Vandiver's conjecture is known for $p < 12,000,000$ (BCEMS).

When $p \nmid h^+$, the group $K_2^M(\mathcal{O}_{F,S}) \otimes_{\mathbf{Z}} \mathbf{Z}_p$ is generated (over \mathbf{Z}_p) by symbols of the form $\{x, y\}$ with $x, y \in \mathcal{C}$.

Unless $h^+ = 1$, it is possible that there could exist $x, y \in \mathcal{O}_{F,S}^\times$ with $x + y = 1$ and $x \notin \mathcal{C}$.

Specialization:

Consider the set of polynomials

$$P = \{X\} \cup \{\Phi_n(X) \mid n \geq 1, n \neq p\}.$$

where $\Phi_n = n$ th cyclotomic polynomial. $R = \mathbf{Z}[X][P^{-1}]$.

$\text{Spec } R = “(\mathbf{G}_m - \mu_{\neq p})_{\mathbf{Z}},”$ where $\mu_{\neq p} =$ non- p th roots of 1.

The surjection $R \rightarrow \mathbf{Z}[\zeta, \frac{1}{p}]$, $X \mapsto \zeta$ induces

$$K_2^M(R) \rightarrow K_2^M(\mathcal{O}_{F,S}).$$

To put bounds on the size of $K_2^M(\mathcal{O}_{F,S})$, one can first try to find solutions of $f + g = h$ with $f, g, h \in R^\times \cap \mathbf{Z}[X]$.

Question. Given $x, y \in \mathcal{C}$ with $x + y = 1$, do there exist $f, g \in R^\times$ with $f + g = 1$?

Some relations in Milnor K_2 :

a. $\zeta^a + (1 - \zeta^a) = 1$

b. $\zeta^a(\zeta^b - 1) + (\zeta^a - 1) = \zeta^{a+b} - 1$

c. $\zeta^{b+f}(\zeta^{b+d} - \zeta^{c+e})(\zeta^a - \zeta^d) + \zeta^a(\zeta^{b+d} - \zeta^{e+f})(\zeta^{b+c} - \zeta^{d+f})$
 $= \zeta^d(\zeta^{a+e} - \zeta^{b+c})(\zeta^{a+b} - \zeta^{e+f})$

d. $(\zeta^{a+b} - 1)(\zeta^{2a} - 1) + \zeta^a(\zeta^a - 1)(\zeta^b - 1)(\zeta^{a+b} - 1) = (\zeta^a - 1)(\zeta^{2(a+b)} - 1)$

e. $\zeta^b(\zeta^{3a} - 1)(\zeta^{a+b} - 1) + (\zeta^a - 1)(\zeta^b - 1)(\zeta^{a+b} - 1)(\zeta^{2a+b} - 1)$
 $= (\zeta^a - 1)(\zeta^{3(a+b)} - 1)$

f. $\zeta^a(\zeta^{4b} - 1)(\zeta^{a+b} - 1)(\zeta^{a+2b} - 1) + (\zeta^a - 1)(\zeta^b - 1)(\zeta^{a+b} - 1)(\zeta^{a+2b} - 1)(\zeta^{a+3b} - 1)$
 $= (\zeta^{2a+4b} - 1)(\zeta^{2a+2b} - 1)(\zeta^b - 1)$

g. $(\zeta^a - 1)(\zeta^{2(a+b)} - 1)(\zeta^{a+c} - 1)(\zeta^c - 1) + \zeta^a(\zeta^a - 1)(\zeta^b - 1)(\zeta^{2c} - 1)(\zeta^{a+b} - 1)$
 $= (\zeta^{a+b+c} - 1)(\zeta^{2a} - 1)(\zeta^c - 1)(\zeta^{a+b} - 1)$

h. $\zeta^a(\zeta^{2b} - 1)^2(\zeta^{a+b} - 1)^2 + (\zeta^a - 1)(\zeta^b - 1)^2(\zeta^{a+b} - 1)^2(\zeta^{a+2b} - 1)$
 $= (\zeta^b - 1)^2(\zeta^{2a+2b} - 1)^2$

Eigenspaces:

$$\Delta = \text{Gal}(F/\mathbf{Q}) \cong (\mathbf{Z}/p\mathbf{Z})^\times$$

$\omega: \Delta \rightarrow \mathbf{Z}_p^\times$, Teichmüller character

For $i \in \mathbf{Z}$, we have idempotents:

$$\epsilon_i = \frac{1}{p-1} \sum_{\delta \in \Delta} \omega(\delta)^{-i} \delta \in \mathbf{Z}_p[\Delta].$$

Given a $\mathbf{Z}_p[\Delta]$ -module A , we define the ω^i -eigenspace of A :

$$A^{(i)} = \langle a \in A \mid \delta a = \omega(\delta)^i a, \delta \in \Delta \rangle,$$

We have an eigenspace decomposition

$$A = \bigoplus_{i=0}^{p-2} A^{(i)}.$$

Cyclotomic p -units:

$$(\mathcal{C} \otimes \mathbf{Z}_p)^{(i)} = \begin{cases} 0 & i \text{ odd}, i \neq 1 \\ \mathbf{Z}/p\mathbf{Z} & i = 1 \\ \mathbf{Z}_p & i \text{ even} \end{cases}$$

For i odd, let $\eta_i \in \mathcal{C}$ with

$$\eta_i \equiv (\zeta - 1)^{\epsilon_{1-i}} \pmod{\mathcal{C}^p}.$$

Then η_i generates $(\mathcal{C}/\mathcal{C}^p)^{(1-i)}$.

For $c \in \mathbf{Z}$ with $p \nmid c$,

$$(\zeta^c - 1)^{\epsilon_{1-i}} \equiv \eta_i^{c^{1-i}} \pmod{\mathcal{C}^p}.$$

Milnor K_2 modulo p :

Vandiver at $p \Rightarrow (K_2^M(\mathcal{O}_{F,S})/p)^- = 0$.

Fix an even integer $k \geq 2$. Let $\alpha, \beta \in \mathcal{O}_{F,S}^\times$.

Set $\{\alpha, \beta\}_k = \text{image of } \{\alpha, \beta\} \text{ in } (K_2^M(\mathcal{O}_{F,S})/p)^{(2-k)}$.

Eigenspace considerations yield

$$\{\eta_i, \eta_j\}_k = 0 \text{ if } i + j \not\equiv k \pmod{p-1}$$

$$\{\zeta, \eta_j\}_k = 0 \text{ for all odd } j$$

Thus, Vandiver's conjecture at p implies that the $\{\eta_i, \eta_{k-i}\}_k$ generate $(K_2^M(\mathcal{O}_{F,S})/p)^{(2-k)}$.

Identities:

One has

$$\{\alpha, \beta\}_k = \sum_{\substack{i=1 \\ i \text{ odd}}}^{p-2} \{\alpha^{\epsilon_{1-i}}, \beta^{\epsilon_{1+k-i}}\}_k.$$

In particular,

$$\{\zeta^a - 1, \zeta^b - 1\}_k = \sum_{\substack{i=1 \\ i \text{ odd}}}^{p-2} a^{1-i} b^{1-k+i} \{\eta_i, \eta_{k-i}\}_k.$$

Applying the relations:

Consider, for example, the relations (d) with $b = 1 - a$ and $p \nmid a - 1, a$:

$$\frac{(\zeta - 1)(\zeta^{2a} - 1)}{(\zeta^a - 1)(\zeta^2 - 1)} - \zeta \frac{(\zeta^{a-1} - 1)(\zeta - 1)}{\zeta^2 - 1} = 1$$

These yield relations on the $x_i = \{\eta_i, \eta_{k-i}\}_k$:

$$\sum_{\substack{i=1 \\ i \text{ odd}}}^{p-2} (1 + (a-1)^{1-i} - 2^{1-i})(a^{1+k-i} - 1)(2^{1+k-i} - 1)x_i = 0 \quad (1)$$

We can calculate the solution space in $\mathbf{F}_p^{(p-1)/2}$ of the equations resulting from (a)–(h) and $x_i = -x_{k-i}$ to bound the p -rank of $(K_2^M(\mathcal{O}_{F,S})/p)^{(2-k)}$.

Except for (73, 38) and (97, 50), the pairs (p, k) on the previous slide are all irregular pairs, i.e., $2 \leq k \leq p-3$ even, $p \mid B_k$, where $B_k = k$ th Bernoulli number.

Exceptional pairs:

If 2 and 3 are squares mod p , there is a solution of the form listed above for $(p, \frac{p+3}{2})$.

(These are not the only exceptional solutions.)

Conjecture. Let $R_1 = \mathbf{Z}[X][P_1^{-1}]$ and $R_2 = \mathbf{Z}[X][P_2^{-1}]$ with

$$P_1 = \{X\} \cup \{\Phi_n(X) \mid n \geq 1\}$$

$$P_2 = \{X\} \cup \{\Phi_n(X) \mid n \geq 1, (n, 6) = 1\}.$$

There do not exist $f \in R_1^\times$ and $g \in R_2^\times$ with $f + g = 1$, $f(1) = 0$, and $g \notin \langle X \rangle$.

Question. For $p = 73$, is $K_2^M(\mathcal{O}_{F,S})^{(36)} \cong \mathbf{Z}/p\mathbf{Z}$?

As for the irregular pairs, we used the relations (1) (for a odd) and the antisymmetry relations to obtain:

Theorem (McCallum-S.). *For all irregular pairs (p, k) with $p < 10,000$, one has*

$$|(K_2^M(\mathcal{O}_{F,S})/p)^{(2-k)}| \leq p.$$

In fact, we computed:

Proposition. *For all irregular pairs (p, k) with $p < 4,000$, one has*

$$|(K_2^M(\mathcal{O}_{F,S}) \otimes \mathbf{Z}_p)^{(2-k)}| \leq p.$$

Relationship with cohomology:

For now, let F be any number field.

Assume $S \supset \{v \mid n \infty\}$ for some $n \geq 1$.

$G_{F,S}$ = Galois group of the maximal extension of F unramified outside S .

Theorem (Tate, Soulé). *There is a canonical isomorphism*

$$K_2(\mathcal{O}_{F,S})/n \xrightarrow{\sim} H^2(G_{F,S}, \mu_n^{\otimes 2}).$$

Assume that $\mu_n \subset F$. Then

$$H^2(G_{F,S}, \mu_n^{\otimes 2}) \cong H^2(G_{F,S}, \mu_n) \otimes \mu_n.$$

Cohomology groups:

$\text{Cl}_{F,S}$ = S -class group of F (class group Cl_F modulo classes of finite primes in S)

$$\text{Br}_S(F) = \ker(\bigoplus_{v \in S} \text{Br}(F_v) \rightarrow \mathbf{Q}/\mathbf{Z})$$

Kummer theory yields an exact sequence

$$0 \rightarrow \text{Cl}_{F,S}/n \rightarrow H^2(G_{F,S}, \mu_n) \rightarrow \text{Br}_S(F)[n] \rightarrow 0.$$

Cup product:

$$H^1(G_{F,S}, \mu_n) \otimes H^1(G_{F,S}, \mu_n) \xrightarrow{\cup} H^2(G_{F,S}, \mu_n^{\otimes 2})$$

Kummer theory yields a natural injection

$$\mathcal{O}_{F,S}^\times / \mathcal{O}_{F,S}^{\times n} \hookrightarrow H^1(G_{F,S}, \mu_n)$$

We define a pairing:

$$(\ , \)_S = (\ , \)_{n,F,S}: \mathcal{O}_{F,S}^\times \times \mathcal{O}_{F,S}^\times \xrightarrow{\cup} H^2(G_{F,S}, \mu_n^{\otimes 2})$$

Theorem (Soulé). *The diagram*

$$\begin{array}{ccc} \mathcal{O}_{F,S}^\times \otimes \mathcal{O}_{F,S}^\times & \xrightarrow{(\ , \)_S} & H^2(G_{F,S}, \mu_n^{\otimes 2}) \\ \downarrow & & \uparrow \wr \\ K_2^M(\mathcal{O}_{F,S})/n & \longrightarrow & K_2(\mathcal{O}_{F,S})/n \end{array}$$

of canonical maps is commutative.

The projection of $(\ , \)_S$ to $\text{Br}_S(F)[n] \otimes \mu_n$ is the sum of norm residue symbols at $v \in S$.

Now take $F = \mathbf{Q}(\mu_p)$ again.

Since $\text{Cl}_{F,S} = \text{Cl}_F$ and $\text{Br}_S(F) = 0$, we have

$$H^2(G_{F,S}, \mu_p^{\otimes 2}) \cong \text{Cl}_F \otimes \mu_p.$$

Vandiver's conjecture implies the following:

Cyclicity conjecture. $(\text{Cl}_F \otimes \mathbf{Z}_p)^{(i)}$ is cyclic for all i .

The cyclicity conjecture was a question of Iwasawa's.

$(\text{Cl}_F \otimes \mathbf{Z}_p)^{(1-k)} \neq 0$ if and only if $p \mid \frac{B_k}{k}$.

Cyclicity conjecture \Rightarrow for (p, k) irregular,

$$(K_2(\mathcal{O}_{F,S})/p)^{(2-k)} \cong \mathbf{Z}/p\mathbf{Z}.$$

A surjectivity conjecture:

Conjecture (McCallum-S.). *The map*

$$(K_2^M(\mathcal{O}_{F,S}) \otimes \mathbf{Z}_p)^+ \rightarrow (K_2(\mathcal{O}_{F,S}) \otimes \mathbf{Z}_p)^+$$

is surjective.

Remarks:

1. If p violates Vandiver's conjecture and one of the even eigenspaces of the p -part of the class group has p -rank ≥ 2 , then the map cannot be surjective on (-1) -eigenspaces.
2. Injectivity: unlikely?
3. One always has $\{\eta_{1-k}, \eta_{2k-1}\}_k = 0$ for (p, k) irregular.

An approach to surjectivity:

Let $H = F(\eta_{p-k}^{1/p})$, an unramified cyclic degree p extension of F .

Let $\text{Gal}(H/F) = \langle \sigma \rangle$ and $N = \sum_{i=1}^{p-1} \sigma^i$, $D = \sum_{i=1}^{p-1} i\sigma^i \in \mathbf{Z}[\text{Gal}(H/F)]$.

\mathfrak{p}_0 prime of H above p , $\Delta_0 =$ subgroup of $\text{Gal}(H/F)$ fixing \mathfrak{p}_0 .

Proposition. *Let (p, k) be an irregular pair with $p \nmid B_{p+1-k}$. Assume $p = \beta^N$, with $\beta \in \mathcal{O}_{H,S}^\times$ such that its image in $\mathcal{O}_{H,S}^\times / \mathcal{O}_{H,S}^{\times p}$ is fixed by Δ_0 . Then*

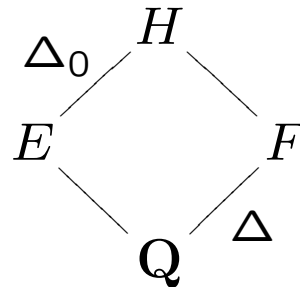
$$(\eta_{k-1}, p)_S \neq 0 \iff (\eta_{k-1}, \beta^D)_{p, H_{\mathfrak{p}_0}} \neq 1 \iff \beta^D \notin H_{\mathfrak{p}_0}^{\times p}.$$

For $p = 37$, this is computationally verifiable.

Theorem (McCallum-S.). *The surjectivity conjecture holds for $p = 37$.*

Sketch of proof.

With the help of W. Stein and C. Fieker, we determined the p -unit group of the fixed field E of Δ_0 as follows.



The field E is generated by the trace x of a 37th root of η_5 , and we found a minimal polynomial for this element using CRT. Various Magma routines then took 5 days on a 2GHz processor to produce an optimal representation of the integer ring of E , from which its p -unit group was computable. One of the p -units β had norm p . By computing the various embeddings of x in the H_p , we were able to verify the condition of the proposition for β^D .

The minimal polynomial of x :

$$\begin{aligned} & x^{37} - 6483584x^{34} - 118234637824x^{33} - 123335506765824x^{32} - 7894900273815552x^{31} \\ & - 25584896141781024768x^{30} - 19612786666813992009728x^{29} - 2221784070205669762924544x^{28} \\ & - 33628014249666292632903483392x^{27} - 4805711697609190244214712041472x^{26} \\ & - 2249002615426863992005848511545344x^{25} - 13099755496539209311468832290825568256x^{24} \\ & - 3171787436319383501703813676940597919744x^{23} \\ & + 476259323830076662111107898811789814530048x^{22} \\ & - 1396232608839552259966984463923520026947092480x^{21} \\ & - 331493134727514939719441018060252656606965137408x^{20} \\ & - 80268638062435074559599184759300711777564488630272x^{19} \\ & - 872057565672136492561824204817812097995282872168087552x^{18} \\ & + 1772659418875854490177280483057352783210247369401565184x^{17} \\ & + 37244222236334875481641252538596552828631758622687299108864x^{16} \\ & - 20651404785477501467881895153357983415526349942938256921329664x^{15} \\ & + 31183544125608715763774641955998078374374445370791241228146966528x^{14} \\ & + 2854705449484624416795330612386811215415869973011706932441160613888x^{13} \\ & - 18557314583560485308211477301528775481854373440798991639264756844462080x^{12} \\ & + 3087405021478910646130093242279350919332930043815268747163999299543498752x^{11} \\ & - 844861169134880185162881813189113039529594781451540816736263726469132320768x^{10} \\ & - 1816305918878969636874702964809165551139833636304814687020499515520778093 \\ & 19936x^9 \\ & + 4849659113957649708716655446098404792782070205898868441096885058833612420 \\ & 49937408x^8 \\ & + 5511404977678219958262233454095746148362443395726320712307332651607429387 \\ & 6028866560x^7 \\ & - 1068505898256327898948966128873297210949111791350824101005198703230324211 \\ & 96184294522880x^6 \end{aligned}$$

+1225313897986066030513017243242734500242304084259199969989081481911199828
 17601008959488 x^5
 +1982469259694895457314935195126430029297012127795195501396552566165464092
 269185291272585216 x^4
 -6606779528917029897795831254093541405143192723743455088686470004371281822
 96246506433818918912 x^3
 -2649881947577745980599970091092292918947828671888834337650679348784388269
 01051317961493560950784 x^2
 +6728762060805419616052269030627338051927895313522501375177099188651104750
 53588494379165834704584704 x
 -26229302920145682793735730674797865320906253597999312333151589937525338452
 7718903616471614294706880512

A better polynomial for E :

$y^{37} + 4y^{36} + 12y^{35} + 36y^{34} - 336y^{33} - 268y^{32} - 3912y^{31} - 7555y^{30} + 60363y^{29} - 254771y^{28} +$
 $1584299y^{27} - 4912687y^{26} + 17776688y^{25} - 51189497y^{24} + 135760742y^{23} - 339845565y^{22} +$
 $729194231y^{21} - 1823351247y^{20} + 2954679204y^{19} - 7136330744y^{18} + 14870105096y^{17} -$
 $19798475744y^{16} + 63485328194y^{15} - 69489469832y^{14} + 240906930339y^{13} - 130150428853y^{12} +$
 $883058481925y^{11} - 525666202335y^{10} + 1336924708802y^9 - 2790390347185y^8 + 2312809893723y^7 -$
 $3005373888911y^6 + 6491297663291y^5 - 2826510585529y^4 + 4902736951337y^3 - 6453741855514y^2 +$
 $3673618997547y - 1546779831802$

The embedding of β^D : $-445 + 13 \cdot 37t - 3t^{31} - 9t^{32} + 18t^{33} + 14t^{34} + 2t^{35} +$
 $O(t^{38}), t = \zeta - 1$

A few consequences for $p = 37$:

The group $K_2^M(\mathcal{O}_{F,S}) \otimes \mathbf{Z}_{37}$ has order 37.

The product maps

$$K_{2i-1}(\mathbf{Z}) \otimes K_{63+72k-2i}(\mathbf{Z}) \rightarrow K_{62+72k}(\mathbf{Z}) \otimes \mathbf{Z}_{37}$$

are nontrivial for a given odd i and any k if $i \not\equiv 5, 27 \pmod{36}$ and nonsurjective otherwise.

(Under the Quillen-Lichtenbaum conjecture, we have surjectivity and triviality in the two respective cases.)

Let M/F be a cyclic extension of degree 37 that is unramified outside 37. Then $|\text{Cl}_{M,S} \otimes \mathbf{Z}_{37}| = 37$ if and only if

$$M \not\subset \mathbf{Q}(\zeta_{37^2}, \eta_5^{1/37}, \eta_{27}^{1/37}).$$

Furthermore, only $M = F(\eta_5^{1/37})$ has trivial 37-class number.

Another approach to surjectivity: $\chi_j: G_F \rightarrow \mathbf{Z}/p\mathbf{Z}$ Kummer character for a p th root of η_j .

Fix i odd and let L be the field defined by χ_i .

Let H be defined by χ_{p-k} .

Then there exists a representation of $G_{\mathbf{Q},S}$ in $\mathrm{Gl}_3(\mathbf{F}_p)$ such that for $\sigma \in G_{F,S}$, we have

$$\rho(\sigma) = \begin{pmatrix} 1 & \chi_i(\sigma) & \kappa(\sigma) \\ 0 & 1 & \chi_{p-k}(\sigma) \\ 0 & 0 & 1 \end{pmatrix}$$

Let M denote the fixed field of the kernel of ρ .

Proposition. *Assume that $(\mathrm{Cl}_F \otimes \mathbf{Z}_p)^{(1-k)}$ is cyclic and that $p \nmid B_{p-i}$. Then $(\eta_i, \eta_{k-i})_S = 0$ if and only if M/HL is completely split at all (any) primes above p .*

Hecke algebras:

Let (p, k) be an irregular pair.

\mathbf{T} = the ordinary cuspidal Hecke algebra (over \mathbf{Z}_p) of weight 2, level p , and character ω^{k-2} .

(By ordinary, we mean the maximal subfactor in which U_p is unit.)

\mathbf{T} is generated by Hecke operators T_l with $l \neq p$ prime and U_p Eisenstein ideal:

$$\mathcal{I} = (U_p - 1) + (T_l - 1 - l\omega(l)^{k-2} \mid l \neq p).$$

Idea: study $Y =$ eigenspace of $H_{\acute{e}t}^1(X_1(p), \mathbf{Z}_p)^{\text{ord}}$ on which $\langle i \rangle$ acts as i^{k-2} for $i \in \mu_{p-1}(\mathbf{Z}_p)$ “modulo \mathcal{I}^2 ”.

The modular representation (following Ohta):

The action of $G_{\mathbf{Q}}$ on Y provides

$$\rho: G_{\mathbf{Q}} \rightarrow \text{Aut}_{\mathbf{T}}(Y).$$

Fix a decomposition group D_p in $G_{\mathbf{Q}}$ at p .

Let I_p be the inertia subgroup of D_p .

Fix $\Delta_p \leq I_p$ with $\omega: \Delta_p \xrightarrow{\sim} (\mathbf{Z}/p\mathbf{Z})^{\times}$.

Under Δ_p , we have $Y = Y^+ \oplus Y^-$.

For $\sigma \in G_{\mathbf{Q}}$, we write

$$\rho(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix},$$

$a(\sigma) \in \text{End}_{\mathbf{T}}(Y^-)$, $b(\sigma) \in \text{Hom}_{\mathbf{T}}(Y^+, Y^-)$, ...

For $\sigma \in I_p$, we have

$$\rho(\sigma) = \begin{pmatrix} a(\sigma) & 0 \\ c(\sigma) & 1 \end{pmatrix},$$

Note: $\text{End}_{\mathbf{T}}(Y^{\pm}) \hookrightarrow \mathbf{T} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$.

For $\sigma, \tau \in G_{\mathbf{Q}}$, we have

$$\begin{aligned} d(\sigma) &\equiv 1 \pmod{\mathcal{I}}, \\ b(\sigma)c(\tau) &\equiv 0 \pmod{\mathcal{I}}. \end{aligned}$$

In fact, let B (resp., C) denote the \mathbf{T} -module generated by all $b(\sigma)$ (resp., $c(\sigma)$) with $\sigma \in G_{\mathbf{Q}}$.

One has $BC = \mathcal{I}$ (Ohta, following Kurihara, Harder-Pink).

Let $\mathfrak{m} = \mathcal{I} + p\mathbf{T}$.

Consider the maps

$$\begin{aligned}\bar{a}: G_{\mathbf{Q}} &\rightarrow (\mathbf{T}/\mathfrak{m})^{\times} & \text{and} & & \bar{b}: G_{\mathbf{Q}} &\rightarrow B/\mathfrak{m}B \\ \bar{c}: G_{\mathbf{Q}} &\rightarrow C/\mathfrak{m}C & \text{and} & & \bar{d}: G_{\mathbf{Q}} &\rightarrow (\mathbf{T}/\mathcal{I}\mathfrak{m})^{\times}\end{aligned}$$

We remark that $\bar{a} = \omega^{1-k}$.

$H =$ fixed field of the kernel of \bar{b} on G_F .

H is an unramified abelian p -extension of F with an ω^{1-k} -action of Galois.

$L =$ fixed field of the kernel of \bar{c} on G_F .

If $p \nmid B_{p+1-k}$, then $L = F(\eta_{k-1})$.

Consider the homomorphism (note: $BC = \mathcal{I}$)

$$\phi_D(\sigma) = \begin{pmatrix} \bar{a}(\sigma) & \bar{b}(\sigma) \\ \bar{c}(\sigma) & \bar{d}(\sigma) \end{pmatrix}.$$

We also have a homomorphism

$$\psi(\sigma) = \begin{pmatrix} 1 & \bar{c}(\sigma) & \bar{d}(\sigma) - 1 \\ 0 & \omega^{1-k}(\sigma) & \bar{b}(\sigma) \\ 0 & 0 & 1 \end{pmatrix}$$

defining the same extension M/HL as ϕ_D .

$\bar{d}(\varphi_p^{-1}) = U_p$ for a Frobenius $\varphi_p \in D_p$

M/HL is non-split at primes above p if and only if

$$\mathcal{I} = \mathcal{I}\mathfrak{m} + (U_p - 1)$$

By the earlier proposition, we have:

Theorem (S.). Assume that $p \nmid B_{p+1-k}$ and $(\text{Cl}_F \otimes \mathbf{Z}_p)^{(1-k)}$ is cyclic. Then $U_p - 1$ generates the group $\mathcal{I}/\mathcal{I}^2$ if and only if $(p, \eta_{k-1})_S \neq 0$.

Theorem (S.). For any irregular pair (p, k) with $p < 1000$, we have $\mathcal{I} = (U_p - 1) + \mathcal{I}^2$.

Corollary. For $p < 1000$, the map

$$K_2^M(\mathcal{O}_{F,S}) \otimes \mathbf{Z}_p \rightarrow K_2(\mathcal{O}_{F,S}) \otimes \mathbf{Z}_p$$

is surjective.

Sketch of proof.

Let \mathcal{H} denote the full cuspidal Hecke algebra for $\Gamma_1(p)$ and ω^{k-2} . We used built-in Magma routines for modular symbols (W. Stein) to compute the U_p and T_i in \mathcal{H} for all i with $1 \leq i < p/6$, viewed in $M_d(\mathbf{Z}_p)$ for some d . These T_i generate \mathcal{H} as a \mathbf{Z} -module. Let \bar{T}_i and \bar{U}_p be the images in $M_d(\mathbf{Z}/p^2\mathbf{Z})$. Let M be the submodule of $M_d(\mathbf{Z}/p^2\mathbf{Z})$ spanned by the \bar{T}_i .

We computed N minimal such that the \bar{T}_i with $1 \leq i \leq N$ generate M . Then p and the $T_i - \sum_{0 < e|i} \omega(e)^{k-2} e$ with $1 \leq i \leq N$ generate \mathcal{I} over \mathbf{Z}_p , provided that

$$\mathcal{H}/\mathcal{I} \otimes_{\mathbf{Z}} \mathbf{Z}_p \cong \mathbf{T}/\mathcal{I} \cong \mathbf{Z}_p/L_p(-1, \omega^k)$$

is p -torsion, which we checked. We computed the images I and J of \mathcal{I} and \mathcal{I}^2 in M using these elements and their products. We verified that $I = J + (\bar{U}_p - 1)$.